Escuela Politécnica Superior

Guía práctica de ciberseguridad en el hogar

Máster Universitario en Ciberseguridad

Trabajo Fin de Máster

Autor:
Pablo Blasco Herrero

Tutor:
José Vicente Berná Martínez

junio 2019

Universitat d'Alacant
Universidad de Alicante

Licencia

Este documento ha sido confeccionado por Pablo Blasco Herrero como trabajo final de máster.

Versión del documento

2019.06.01

Licencia

Se permite la reproducción, distribución y comunicación pública de la obra, incluso con fines comerciales siempre y cuando reconozca y cite la obra de la forma especificada por el autor o el licenciante.

Resumen

Las nuevas tecnologías e Internet han traído incontables oportunidades de ocio, aprendizaje y compartición de información impensables hace unos años, pero que esconden una terrible realidad: no están exentas de amenazas, y es necesario tener un mínimo de conocimientos de seguridad para poder utilizar sin riesgos la red de redes.

Como sucede con toda revolución tecnológica, hay mucha gente que no puede seguir el ritmo de evolución, lo que conlleva que hagan uso de Internet (imprescindible para cada vez un mayor número de acciones del día a día) pero sin los conocimientos para poder hacerlo de una manera segura. Como he podido comprobar de primera mano con mis padres, cada vez que estos usuarios tratan de ponerse al día se ven abrumados por la cantidad de noticias e información, y a menudo se encuentran perdidos. Estos sectores de la población, junto con los menores, son los más vulnerables.

El presente trabajo se inspira en mis padres e hijos, y trata de facilitar el aprendizaje mínimo de seguridad a usuarios que, como ellos, tienen un conocimiento que les permite utilizar dispositivos electrónicos e Internet, pero serían víctimas de cualquier ataque, por poco sofisticado que fuera.

Para ello, realizo en primer lugar un análisis teórico del riesgo mediante la metodología Magerit, tal y como hemos visto en “Sistemas de Gestión de la Seguridad”, aunque adaptándola a la realidad de un entorno doméstico en el que existen diferencias fundamentales con el entorno empresarial para el que se define, aunque siguiendo sus pasos fundamentales:

1. Selección de activos a proteger, que incluye tanto los activos habituales en el entorno empresarial (ordenadores, información, etc.) como los miembros del hogar y en especial los menores.
2. Identificación de amenazas para cada uno de los activos.
3. Cálculo del riesgo derivado de las amenazas.
4. Propuesta de salvaguardas para mitigar las amenazas.
5. Cálculo del riesgo residual, para que quede por debajo del umbral de riesgo aceptable.

Una vez completado el análisis, he generado unas fichas con un lenguaje lo más sencillo posible, donde explico a los usuarios las amenazas y que medidas deben introducir para protegerse de las mismas. La parte correspondiente a la educación de los usuarios es la que he considerado más importante, y se incluye también enlaces a recursos online de probada reputación, a fin de

que los usuarios puedan profundizar más sus conocimientos una vez se vean cómodos con los contenidos de la guía.

Dicha guía ha sido distribuida entre familiares, amigos y una asociación de la que soy miembro y, como podía esperarse, la acogida ha sido desigual:

- Los usuarios con conocimientos más avanzado esperaban una mayor profundidad y la inclusión de medidas de protección más avanzadas
- Los usuarios menos expertos me han confesado que tienen dificultades con varios de los conceptos y salvaguardas, aunque la encuentran muy interesante y adecuada.

Me considero, por tanto, satisfecho con el resultado, dado que el público objetivo de la misma la valora positivamente, pero con puntos que les obligan a aprender y poner en práctica conceptos y medidas nuevas.

Motivación, justificación y objetivo general

Mi objetivo principal con la realización de este Máster Universitario en Ciberseguridad siempre ha sido profesional: mejorar mis conocimientos en este ámbito del conocimiento de cara a poder ser un mejor ingeniero y de esa manera tener un mejor desempeño en mi puesto de trabajo, en el que llevo un par de años dedicándome a mejorar la seguridad de los productos que desarrollamos como arquitecto de seguridad.

Al mismo tiempo, 2 objetivos secundarios han influido mucho en que me decidiera a realizar el importante esfuerzo que conlleva la realización de un Máster Universitario mientras sigo teniendo un trabajo a jornada completa:

1. Aunque llegué de rebote a este mundo, cuando en mi empresa me ofrecieron el puesto de arquitecto de seguridad, he descubierto que es un tema que me apasiona, y trato de dedicar todo el tiempo que me es posible a aprender más, ya que cuanto más aprendo más veo que lo que conocía hasta hace un par de años no era más que la punta del iceberg.
2. Como todo profesional, aspiro a mejorar mi situación laboral y estar cualificado para poder ocupar puestos que conlleven un mayor reconocimiento, y eso en una empresa como la mía que se dedica al mundo de la identidad digital y la seguridad pasa por ampliar mis conocimientos en ciberseguridad.

Cuándo nos comentaron que había que elegir el Trabajo de Fin de Máster y que podíamos proponer nosotros trabajos adicionales a los ofertados, mi primera impresión fue de sorpresa, ya que pensaba que (al estar programado para el segundo cuatrimestre) no nos comentarían nada sobre el mismo hasta ese momento, en el que apenas habíamos iniciado las clases y todavía trataba de encajar mi planificación semanal para poder completar las distintas tareas que empezaban a acumularse: ¿Cómo iba a poder encajar el desarrollo del TFM y arañar algo de tiempo cuándo a duras penas me mantenía a flote?

Al mismo tiempo, y casi de manera instantánea, me vino a la cabeza la idea de un proyecto que hacía tiempo venía rondándome la cabeza, aunque la pereza o mejor dicho la no asignación de una alta prioridad hacía que siempre lo relegara o cumpliera con lo mínimo que ya conocía: conseguir proteger de manera eficiente y eficaz el entorno digital de mi propia casa.

Esta vez, sin embargo, confluían diversos factores adicionales que encajaban perfectamente:

- A diferencia de en momentos anteriores, mis dos hijos están interactuando con dispositivos electrónicos y con Internet, lo cual venía elevando poco a poco la prioridad de empezar esta tarea.
- Cada vez más, noto que mucha gente (entre la que se incluyen mis padres) acude a mí para resolver cuestiones relacionadas con la seguridad. Siendo sinceros, los informáticos siempre recibimos preguntas de todo tipo relacionadas con cualquier tecnología (desde poner en hora el horno a qué teléfono maravilloso podemos recomendar que sea de gama alta y cueste 'no más de 150-200 €'), pero vengo notando que la brecha entre los conocimientos específicos que hay que tener y los que tiene la mayoría de la gente no para de aumentar, y se encuentran más perdidos que nunca ante las noticias que les bombardean en los telediarios sobre cibercrímenes.
- Pese a que llevábamos pocas sesiones, la asignatura de 'Sistemas de Gestión de la Seguridad' nos había introducido en las (hasta entonces desconocida para mí) metodología formal empleada en las empresas para controlar los posibles problemas de seguridad. Esto resolvía uno de los mayores inconvenientes que siempre me habían llevado a retrasar el proyecto, al permitirme realizar una evaluación de la seguridad en la que no me limitara a incluir aquellas medidas de protección y procedimientos que se me pudieran ocurrir, sino que estuviera seguro de abordar todos los aspectos relevantes.

Juntando todo lo anterior, y la verdad sin pararme a pensar demasiado en todas las posibles derivaciones, me animé a hablar con José Vicente para comentarle lo que venía pensando: ¿Es posible mejorar la seguridad de un hogar utilizando la metodología formal que se aplica en la empresa? ¿Sería posible obtener un resultado que no fuera válido únicamente para personas con amplios conocimientos informáticos, sino que pueda ser entendido y utilizado por personas que carecen de ellos como pueden ser mis padres?

A lo largo del desarrollo de este Trabajo de Fin de Máster, está claro que aprenderé alguna cosa nueva que me ayude a título individual, pero creo que, si consigo llevarlo a buen puerto, sobre todo me permitirá devolver a la sociedad (empezando por ese entorno muy cercano que son la familia y los amigos) parte de mis conocimientos para permitirles vivir en un entorno más seguro.

Agradecimientos

En primer lugar, me gustaría agradecer a mi esposa Esther por su apoyo, comprensión y esfuerzo sin el cual habría sido materialmente imposible la realización de este Máster Universitario. He tenido que robar muchas horas a mi aportación en el entorno doméstico, y ella siempre ha estado allí realizando un esfuerzo extra para suplir estos huecos. Al mismo tiempo, ha tenido que soportar pacientemente mis quejas, cambios de humor y cansancio, y lo ha hecho siempre con una sonrisa, animándome cada vez que lo necesitaba. Por último, y no menos importante, ha sido la sufrida revisora principal de este trabajo y ha tenido que responder mis incesantes preguntas, aportando el punto de vista de alguien que no es experto en tecnología imprescindible para conseguir acercarlo a un lenguaje comprensible para todo el mundo.

También quiero agradecer a todos aquellos familiares y amigos que han contestado a mis preguntas, y quiero librarles de responsabilidad en el trabajo final: si algo no resulta útil es por mi incapacidad de trasladar sus comentarios, y no por su falta de interés o claridad.

Me gustaría agradecer a la empresa en la que trabajo, Gemalto, tanto el descubrimiento del mundo de la ciberseguridad como el apoyo que he recibido en todo momento para la realización de este Máster Universitario, al adaptarme mi horario y carga laboral para poder acudir a las clases presenciales, financiarme parte de este y ayudarme en todas las cuestiones que estaba en su mano, tanto a nivel general como muy particular por parte del departamento de Recursos Humanos.

Por último, pero no menos importante, quiero agradecer al tutor de este Trabajo de Fin de Máster, José Vicente Berna Martín, su guía y ayuda necesaria para poder plasmar los objetivos un tanto subjetivos en un trabajo concreto.

Citas

Cualquier tecnología suficientemente avanzada es indistinguible de la magia.

Arthur C. Clarke

Vive como si fueras a morir mañana; aprende como si el mundo fuera a durar para siempre.

Mahatma Gandhi

Las matemáticas son el alfabeto con el cual Dios ha escrito el Universo.

Galileo Galilei

Índice de contenidos

Índice de Ilustraciones

Índice de tablas

1. Introducción

El presente Trabajo de Fin de Máster se encuentra a caballo entre los dos mundos que componen mi vida, y de la mayoría de las personas.

Por un lado, tiene sus raíces en el mundo profesional y trata de hacer valer tanto mis conocimientos previos como todo aquello que he aprendido a lo largo del Máster. Esto incluye herramientas y procedimientos desarrollados y perfeccionados en el ámbito laboral a la hora de realizar una gestión de los riesgos (relacionados con la seguridad) a los que toda empresa se está expuesta.

Por otro lado, intenta aplicar dichos conocimientos, herramientas y procedimientos a un entorno personal, utilizándolos para realizar una gestión adecuada de los riesgos de seguridad a las que todos los hogares se enfrentan en mayor o menor medida.

Dicho espacio personal podría abarcar personas con cualquier grado de conocimientos previos en la materia, pero el enfoque que quiero dar al mismo es de que sea útil precisamente a aquellos hogares en los que no hay un experto que sea capaz de entender y trasladar las medidas de protección más complejas, puesto que son estos los que habitualmente se encuentran más indefensos.

Decidir esta línea de actuación conlleva unas implicaciones muy profundas en todo el trabajo, puesto que al final voy a tener que centrarme en aquellos activos más habituales en este tipo de entornos menos tecnológicos y al mismo tiempo ser capaz de desarrollar un conjunto de recomendaciones que puedan ser entendidas y llevadas a la práctica por personas poco habituadas la puesta en marcha de políticas de seguridad.

El presente Trabajo de Fin de Máster tendrá por lo tanto dos elementos muy diferenciados

- Por un lado, una valoración formal de los activos, amenazas, riesgos y medidas a implantar.

Por el otro, una traslación de las medidas seleccionadas a un lenguaje llano y entendible, en un documento que pueda distribuirse y ser útil a familiares y amigos.

2. Estudio de viabilidad

Para evaluar la viabilidad del proyecto, voy a realizar un análisis DAFO recogido en la Tabla 1.

Tabla 1. DAFO de viabilidad
(Fuente: propia)

	Positivo	Negativo
Origen Interno	• Conocimiento sobre ciberseguridad. • Interés personal. • Experiencia en la gestión de proyectos.	• Tiempo disponible. • Conocimientos sobre la preparación de materiales para difusión a personas no técnicas.
Origen Externo	• Apoyo del tutor del TFM. • Apoyo de mi empresa a la realización del Máster. • Recursos sobre ciberseguridad disponibles.	• Usuarios finales de la guía con conocimientos muy diversos, y a veces ajenos al mundo tecnológico. • Imposibilidad de trasladar todas las medidas a un lenguaje entendible. • Capacidad de atención y esfuerzo de usuarios finales limitada / muy limitada. • Existencia de una infinidad de activos y situaciones particulares.

A la vista de la matriz, puedo extraer las siguientes conclusiones sobre la viabilidad del proyecto:

- La limitación en tiempo de desarrollo del TFM unida a la limitada capacidad de esfuerzo de los usuarios finales y junto a la amplia variedad de entornos domésticos llevan a tener que tomar la aproximación de seleccionar muy cuidadosamente los activos y las medidas a incorporar en el presente trabajo, a fin de no tener el resultado contraproducente de que dichos usuarios finales descarten la guía por tener esta excesiva longitud o complejidad.
- Dada la capital importancia de la sencillez, en algunos casos puede ser necesario no incluir alguna medida seleccionadas si no hay manera de poder presentarla de una manera sencilla y concisa, pudiendo optar por incluir algunos enlaces a documentación existente para aquellos usuarios más avanzados.
- A fin de evaluar la usabilidad de la guía, va a ser necesario hacer circular las distintas medidas entre familiares y amigos (como representantes de los distintos grados de conocimiento) para seleccionar aquellas medidas y/o redacciones que facilite el entendimiento, y por lo tanto la difusión, de la guía.

Por tanto, a modo de resumen, no albergo dudas sobre la viabilidad del proyecto, aunque sí que las tengo sobre si va a ser posible cumplir el (ambicioso) objetivo de que la guía resultante sea entendible por la gran mayoría de los usuarios finales.

3. Planificación

Mi objetivo temporal es ser capaz de presentar el TFM en la convocatoria de junio, que implica la entrega de la versión final del presente TFM durante la primera semana de junio. Con el fin de hacer frente a las distintas contingencias que puedan ocurrir, voy a fijarme un calendario que planifique la finalización a mediados de mayo, de manera que quede un pequeño colchón temporal para dichos imprevistos.

Durante el primer cuatrimestre, he realizado diversas actividades relacionadas con el presente proyecto, desde leer mucha información sobre el estado del arte a realizar un diseño mental de cómo llevar el proyecto a buen puerto, pero la verdad es que casi nada de este trabajo ha quedado reflejado más que en apuntes y notas que sirven como punto de partida pero que no pueden considerarse como apartados finalizados, por lo que me va a tocar apretar los plazos como queda recogido en la Tabla 2.

Tabla 2. Planificación temporal TFG para entrega en junio
(Fuente: propia)

Contenidos	**Tiempo total**	**Fecha límite fin**
Recopilación documentación	4 meses	1 marzo
Motivación, justificación, objetivo general Introducción Estudio de viabilidad Planificación	2 semanas	15 marzo
Estado del arte Objetivos Metodología	2 semanas	31 marzo
Análisis formal Selección contenidos a tratar en la guía	2 semanas	15 abril
Redacción contenido guía Encuestas usuarios	2 semanas	30 abril

Resultados Conclusiones y trabajo futuro Resumen Referencias, bibliografía y apéndices Agradecimientos, citas, índices	2 semanas	15 mayo

A modo de control, he realizado también una segunda planificación que implique retrasar la entrega a la siguiente convocatoria, de manera que sirva para ir viendo cuando un posible retraso desde la planificación original haga recomendable un cambio de objetivo temporal, apoyado a su vez por la mayor disponibilidad temporal una vez se haya finalizado la docencia, entregas y exámenes del segundo cuatrimestre. En este posible escenario, ajusto los plazos para terminar antes de las vacaciones de agosto, lo que me lleva a la planificación mostrada en la Tabla 3.

Tabla 3. Planificación temporal TFG para entrega en septiembre
(Fuente: propia)

Contenidos	**Tiempo total**	**Fecha límite fin**
Recopilación documentación	4 meses	1 marzo
Motivación, justificación, objetivo general Introducción Estudio de viabilidad Planificación	1 mes	31 marzo
Estado del arte Objetivos Metodología	1 mes	30 abril

Análisis formal Selección contenidos a tratar en la guía	1 mes	31 mayo
Redacción contenido guía Encuestas usuarios	1 mes	30 junio
Resultados Conclusiones y trabajo futuro Resumen Referencias, bibliografía y apéndices Agradecimientos, citas, índices	1 mes	31 julio

4. Estado del arte

Dada la doble vertiente del presente TFM, voy a distinguir claramente entre ambas a la hora de tratar de plasmar la información existente.

4.1. Ámbito empresarial.

Existen multitud de marcos formales empresariales para el análisis y gestión de riesgos. Dado que dicho análisis no corresponde con el núcleo del presente proyecto y que además voy a hacer un uso parcial del mismo, utilizando únicamente aquellos recursos que van a tener una aplicación en el ámbito doméstico y vayan a poder ser gestionados y comprendidos por la mayoría de los usuarios, voy a decantarme por utilizar el mismo que hemos visto en la asignatura de Sistemas de Gestión de la Seguridad: Magerit [1].

De acuerdo con su entrada en la Wikipedia [2] “Magerit es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica del gobierno español para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas.”.

Dicha metodología permite saber el valor de los activos digitales (tanto información como servicios digitales) y seguir un proceso para conocer el riesgo de cada uno de dichos activos de cara a poder gestionarlos de manera metódica, de tal manera que diversos analistas con distintos conocimientos produzcan un resultado (idealmente) igual.

El análisis y gestión de riesgos se encuentra regulado para la administración electrónica en el Real Decreto 3/2010 [3], pero es habitual su uso en un ámbito empresarial dado que hay disponible una documentación extensa de la metodología y herramientas construidas por diversos actores, por lo que se ha convertido en uno de los marcos más extendidos dentro de España.

La Ilustración 1 expone los elementos que componen el análisis de riesgo.

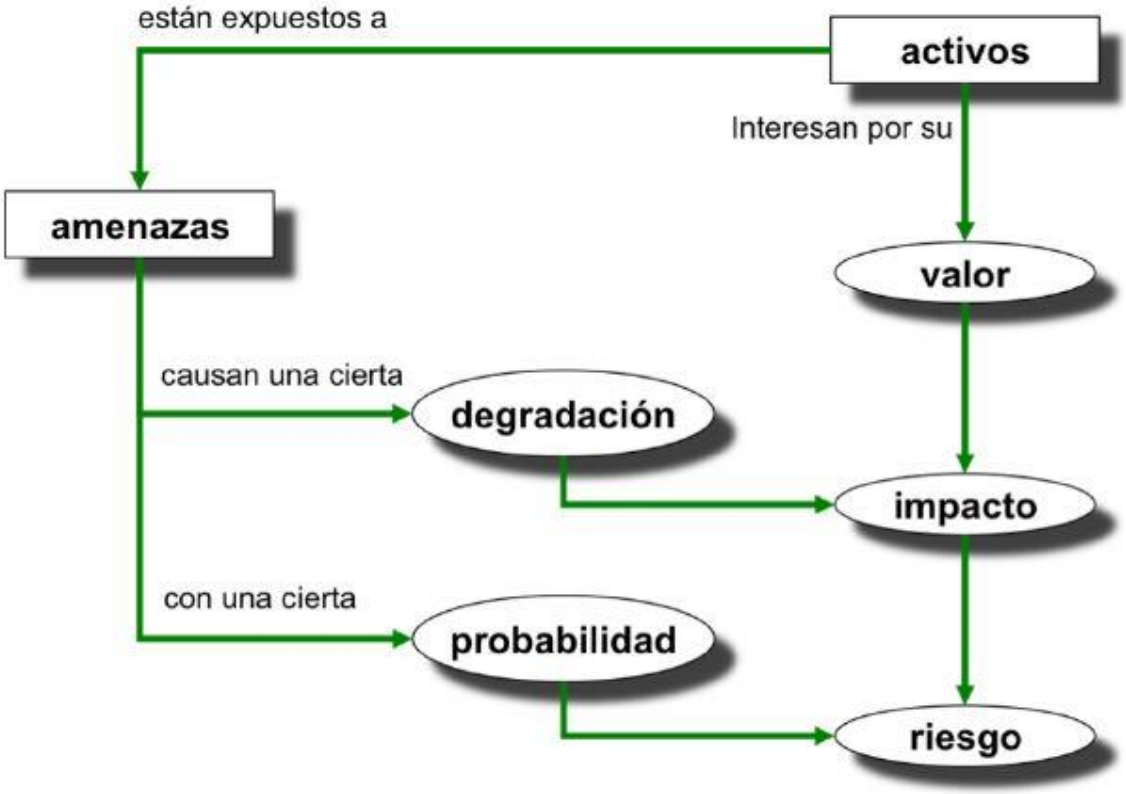

Ilustración 1. Análisis de riesgo.
(Fuente: Tema 3 – Sistemas de Gestión de la Seguridad [4])

El análisis de riesgo comprende las siguientes etapas

1. Obtención del catálogo de activos.
2. Identificación y análisis de las amenazas.
3. Cálculo del impacto de las amenazas.
4. Cálculo de la probabilidad de las amenazas.
5. Cálculo del riesgo

A fin de proteger los activos, se utilizan salvaguardas para disminuir la degradación producida por una amenaza o la probabilidad de esta, de tal manera que se disminuya el impacto y/o el riesgo, como refleja la Ilustración 2, que corresponde a la gestión del riesgo.

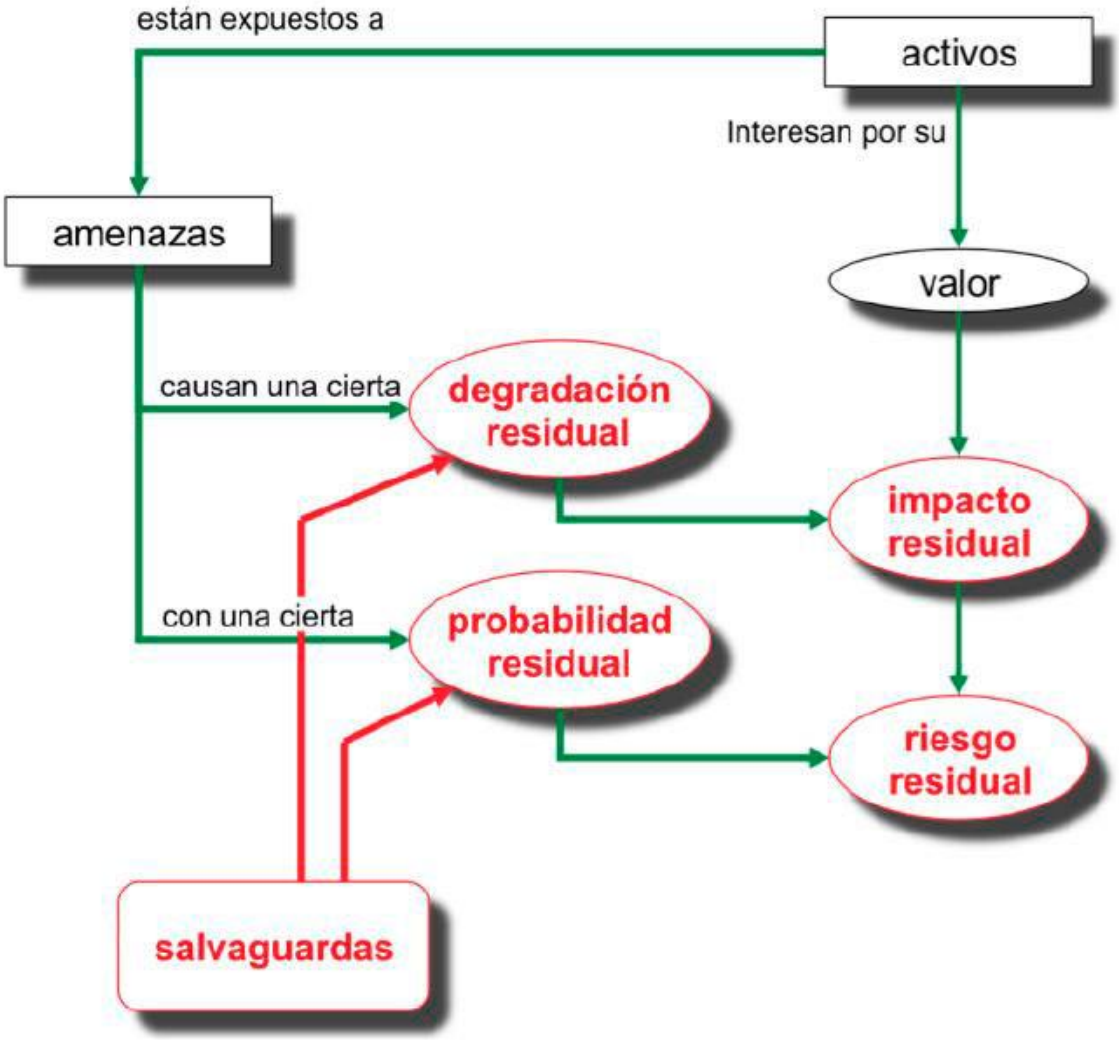

Ilustración 2. Salvaguardas.
(Fuente: Sistemas de Gestión de la Seguridad [5])

Lo que Magerit nos ofrece es (además de instrucciones claras sobre cómo realizar el proceso descrito) un catálogo completo de los activos, amenazas y salvaguardas más habituales, así como de metodologías para estimar el valor de los distintos activos, así como de la degradación, probabilidad y riesgo de las distintas amenazas.

Se trata, por tanto, de un entorno donde la información, procedimientos y concienciación se encuentran en un nivel muy elevado.

4.2. Ámbito doméstico.

Existe una amplia variedad de fuentes orientadas al usuario doméstico, por lo que el presente trabajo no va a tratar de abarcar todas ellas, sino que me he centrado en las que he considerado más relevantes, realizando un pequeño análisis de las mismas en el que primará la comprensibilidad y aplicabilidad de dicha información para usuarios que en la mayoría de las

ocasiones no son expertos en la materia por lo que las explicaciones deben de ser muy claras y concisas, además de utilizar un lenguaje llano que no pretenda causar alerta ni nerviosismo entre los lectores. Al mismo tiempo, voy a descartar las fuentes en idiomas que no sean el castellano por no ser accesibles a toda la población, y especialmente a los usuarios con menos bagaje en Internet, menos acostumbrados al acceso a contenido en otros idiomas y al uso de los traductores en línea.

La Tabla 4 resume los criterios de evaluación más relevantes para el presente TFM que serán utilizados, tras analizar cada fuente de manera aislada, a fin de realizar un análisis comparativo de dichas fuentes de acuerdo con los criterios expuestos.

Tabla 4. Aspectos relevantes para la evaluación de las fuentes de información (Fuente: propia)

Criterio	**Definición**
Usuarios objetivo	Característica principal de los usuarios objetivo de la fuente.
Nivel mínimo usuarios	Nivel de conocimientos informáticos que deben tener los usuarios para comprender el contenido.
Orientación	Área de la seguridad / tipo de información en la que se centra.
Objetivo	Denota el objetivo principal de la fuente: - Divulgación, cuando trate de expandir el conocimiento de los usuarios con información, tratando de mantenerlos al día. - Educación - NA (No Aplicable), en otros casos.
Completitud contenidos	Gradúa si los contenidos presentes satisfacen el objetivo principal de la fuente.
Claridad contenidos	Valora como de accesible es el contenido a un usuario con bajos conocimientos informáticos / de ciberseguridad. Se tiene en cuenta aspectos como la claridad, vocabulario u organización de la explicación.
Organización contenidos	Valora la accesibilidad de los contenidos para los usuarios. Se tiene en cuenta aspectos como la existencia de un menú de

	temas, capacidad de búsqueda por palabras clave o la usabilidad de la fuente.
Contenidos actualizados	Valora que los contenidos de la fuente estén al día / sean relevantes.

Una al día

"Una al día" [6] Boletín diario de información de noticias de seguridad informática en castellano, publicado de manera voluntaria y gratuita por empleados de la primera empresa de ciberseguridad en España (HISPASEC SISTEMAS S.L.) desde octubre de 1998.

Las noticias son publicadas de múltiples maneras (blog, cuenta Twitter, correo electrónico, Facebook, LinkedIn) y el sitio web incluye un catálogo completo de las noticias publicadas hasta la fecha, ordenada por temáticas para facilitar su consulta.

Su objetivo principal es la divulgación y concienciación de los usuarios, y las noticias tienen un amplio espectro de temáticas, desde asuntos relevantes desde un punto de vista doméstico a explicaciones sobre brechas de seguridad o análisis de marcos de seguridad.

No se puede, por tanto, decir que es un recurso que esté destinado a usuarios inexpertos, aun cuando algunas de las noticias sí que pueden interesarles e incluso estar escritas de una manera comprensible a estos, dado que un amplio porcentaje de las noticias necesita de un nivel mínimo de conocimientos informáticos (generales o relacionados con la seguridad), por lo que los usuarios inexpertos rápidamente perderán el interés en esta fuente.

INCIBE

El Instituto Nacional de Ciberseguridad (INCIBE) [7][8], sociedad dependiente del Ministerio de Economía y Empresa, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos. Para realizar esta labor se centra en 3 pilares: servicios de ciberseguridad, tecnologías de ciberseguridad y apoyo a la industria. Dispone de canales de comunicación independientes para los ciudadanos y para las empresas, y los relevantes para el presente estudio son la "Oficina de Seguridad del Internauta (OSI)" [9] y el "INTERNET SEGURA FOR KiDS (IS4K)" [10].

Nos encontramos por tanto ante dos recursos cuya orientación principal es hacia usuarios domésticos, segmentando el contenido destinado hacia los niños en una web específica.

Oficina de Seguridad del Internauta

Web en castellano con múltiples funcionalidades orientadas a usuarios con niveles de conocimiento variable, pero ofreciendo mucha información clara, accesible y dirigida a aquellas personas con menor nivel informático.

Dado que el enfoque de esta coincide plenamente con el objetivo del presente TFM, realizo un análisis más exhaustivo de este recurso.

Dispone de los siguientes elementos principales:

- Avisos de seguridad muy bien elaborados, donde se incluyen múltiples apartados (recursos afectados, solución, detalles y referencias) donde se usa un lenguaje claro y entendible que permite a casi cualquier usuario identificar si el problema le afecta y como solucionarlo o donde acudir para obtener más ayuda. Altamente recomendables para aquellos usuarios domésticos que quieran mantenerse al día de las nuevas amenazas de seguridad.
- Blog con 2-3 entradas mensuales donde se tratan temas con mayor profundidad, con un fin de divulgación sobre asuntos de seguridad generales como puede ser enseñar a los usuarios a generar contraseñas robustas, el uso del doble factor de autenticación o como mejorar la seguridad de nuestros datos. Muy recomendable para usuarios con un nivel de conocimientos de seguridad básicos que quieran mejorarlo.
- Historias reales, con una periodicidad mensual, en la que las entradas de amplia extensión desarrollan una historia centrada normalmente en una familia cibernauta ficticia que comete un error habitual (como puede ser clicar en un mensaje de phishing y proporcionar datos personales), aunque a veces se trata de casos reales (suplantación digital, caer en una estafa digital, etc.). La explicación de los hechos está muy bien redactada para poder ser comprendida por todo el mundo, e incluye indicaciones de qué se ha hecho mal en cada caso y como tendrían que haber actuado los protagonistas de la historia. La manera correcta de actuar no siempre es algo que todos los usuarios podrían hacer como ayuda (por ejemplo: conocer los requisitos que debe cumplir toda entidad que quiera ofrecer un préstamos en España, como estar registrada en Registro de Intermediarios Financieros de la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición), pero dichas explicaciones detalladas si pueden ser muy útiles como consulta por aquellas personas que tengan sospechas de que alguno de los servicios que les ofrecen son

fraudulentos o dudas sobre si tiene que dar la información que les están solicitando, dado que en catálogo de entradas pasadas se puede encontrar una temática muy variopinta y es fácil que haya alguna que guarde bastantes similitudes. Lamentablemente, los cibercriminales son conscientes de la existencia de este tipo de recursos, por lo que suelen tratar de obtener una respuesta rápida de manera que los usuarios no puedan reflexionar sobre lo que están a punto de hacer o reciban el consejo de algún experto.

- Campañas: paneles digitales que abarcan diversos aspectos de un mismo tema, con enlaces a diversos materiales como pueden ser videos, blogs e infografías para tratar diversos aspectos relacionados con el tema del panel. En estos momentos hay 4 paneles sobre la ciberdelincuencia, los dispositivos IoT, las redes sociales y la seguridad de las contraseñas. Se tratan de un buen recurso para profundizar por parte de usuarios que quieren incrementar su conocimiento sobre dichos temas, o que quieran consultar una duda concreta.
- Páginas donde se recopila información sobre temas que afectan a los usuarios
    - Protección de algunos elementos del hogar (conexión Wifi y los dispositivos móviles), muy completa y entendible en el caso de la Wifi, pero incompleta en el caso de los dispositivos móviles donde quedan áreas por cubrir y la organización de la información puede hacer que ciertos usuarios no consideren que todos los puntos incluidos les interesa.
    - Salvaguarda de la información: privacidad, gestión de contraseñas y copias de seguridad y cifrado de datos. Guías completas y muy recomendables, orientadas a los usuarios con menos conocimientos.
    - Precauciones a la hora de realizar diversas actividades online como puede ser navegar, comprar o uso de redes sociales. Muy completas y con un lenguaje muy entendible. El único pero que se puede poner es que (aunque muy fáciles de seguir por parte de cualquier usuario con una mínima experiencia) puede suponer demasiada información para un usuario inexperto.
    - Explicación de los fraudes más habituales: cómo funciona, cómo reconocerlos, qué hacer si lo detectas a tiempo y (muy importante) qué hacer si te das cuenta tarde de que se trata de un fraude. Nuevamente nos encontramos ante unos recursos muy bien estructurados que permiten tanto concienciar a los usuarios como enseñarles a actuar en cualquier fase

del engaño, con indicaciones claras y concisas que incluyen los contactos en los que apoyarte para consultar, denunciar o aprender más al respecto.

- Guía de privacidad y seguridad en Internet [11]: documento con 18 fichas de una página en la que se abordan 18 temas con unas explicaciones muy visuales y sin profundizar demasiado, pero con enlaces a páginas que desarrollan en profundidad los temas, por lo que se trata de un recurso perfecto para transmitir una información básica a los usuarios noveles y al mismo tiempo permita a un usuario intermedio el seguir esos enlaces para aprender más sobre el tema.
- Guía de compra segura en Internet [12]: La organización del contenido es diferente a la guía anterior, pero no así la claridad y sencillez de las explicaciones que siguen siendo plenamente entendibles por la mayoría de los usuarios. En este caso la información se organiza temporalmente, agrupando primero todas las recomendaciones a realizar antes de comenzar la compra en una web determinada (dispositivo a usar y su configuración, configuración de la red, comprobación del comercio, asegurar el uso de HTTPS, etc.), durante la compra (información relativa a los distintos medios de pago y a como configurar correctamente la cuenta de usuario) y los puntos relevantes tras completar la compra (garantía, gastos de envío, reclamaciones, etc.). Muy recomendable, pero, como en algunos casos anteriores, la extensión del documento (32 páginas en total) va a causar que muchos usuarios desistan de su lectura. Existe un segundo formato [13] en el que la información principal se presenta como una serie de 7 fichas con la información más importante presentada de una manera mucho más visual y con enlaces a páginas web para profundizar sobre los distintos aspectos, que considero mucho más adecuada para los usuarios con menores conocimientos, a fin de no desbordarles con información.
- Enlaces a herramientas de seguridad gratuitas (propias o de terceros) categorizadas para una fácil búsqueda, lo que facilita a los usuarios la selección de la herramienta adecuada una vez se haya convencido de la necesidad de instalarla.

En resumen, una web con una gran cantidad de recursos orientada a la ciberseguridad en el hogar, pero sin un índice claro que permita a los usuarios menos expertos elegir un camino de navegación o un orden de implantación de las distintas medidas de acuerdo con el riesgo relativo de las distintas amenazas.

Al mismo tiempo, a título completamente personal, creo que no tiene la difusión que se merece dado que en muy pocas ocasiones he oído hablar de la Oficina de Seguridad del Internauta.

INTERNET SEGURA FOR KiDS

Web en castellano [10] centrada en la protección de los menores. Tiene por objetivo la promoción del uso seguro y responsable de Internet y las nuevas tecnologías entre los niños y adolescentes. Trata, por tanto, no solo aspectos de ciberseguridad sino también de diversos problemas del mundo real que tienen su contrapartida en el digital como podría ser el ciberacoso o la publicidad en Internet.

Contiene una amplísima cantidad de contenido estructurado y accesible de varias maneras para facilitar su localización.

A través del menú superior se puede acceder a los siguientes elementos:

- Blog con aproximadamente dos entradas por mes donde se tratan diversos temas que van desde la explicación de un mecanismo de seguridad o control de nuestros dispositivos hasta ayuda a los padres a la hora de decidir si ha llegado el momento adecuado para que nuestros hijos dispongan de su primer móvil, o qué aspectos tener en cuenta a la hora de comprar juguetes conectados. Las explicaciones me han parecido muy completas y entendibles, explicando claramente las problemáticas y los aspectos para tener en cuenta. Dada la casi infinita variedad de temas que se podrían tratar, la única pega que veo es la falta de más entradas, problema que se ve acentuado con el limitado tiempo de vida que tienen los artículos más tecnológicos.
- 9 artículos más extensos sobre problemáticas muy habituales y que nos preocupan a todos los padres en un momento u otro del desarrollo de nuestros hijos: privacidad, sexting, ciberacoso, acceso a contenido inapropiado, comunidades de usuarios peligrosas para niños o adolescentes, uso excesivo de las TIC, mediación parental, uso y configuración segura de los dispositivos, grooming. Me parecen que estos artículos son de lectura obligatoria para todo padre a cargo de menores, ya que su orientación y profundidad nos dotan de recursos para poder proteger a nuestros hijos y (lo más importante) para permitirnos transmitirles los conocimientos de cara a que ellos solos puedan hacerse cargo de su protección una vez tengan la madurez necesaria.
- Análisis de las herramientas de control parental existentes, de cara a poder proteger y gestionar la actividad de los menores en Internet y/o con los dispositivos móviles.
- Diversos materiales didácticos adaptados a los menores, recursos y juegos con los que conseguir educar a los menores con respecto a los peligros del mundo digital y como deben actuar en dicho entorno.

- Programas y campañas, más orientados a su uso por parte de los educadores en un ámbito escolar.

Otra clasificación de contenidos, mediante la que se puede acceder a ciertos contenidos enumerados anteriormente, a partir del ámbito, relacionado con los menores, de quien está accediendo a este espacio web

- Familias: se encuentran las guías más relacionadas con un entorno doméstico
    - Guía de juguetes conectados [14]: fichas muy visuales y entendibles sobre diversos aspectos de los juguetes conectados: qué son, qué datos pueden recoger, qué riesgos conllevan, cómo elegirlos, cómo configurarlos, cómo enseñar a jugar. Muy recomendable leerlo si se piensa adquirir uno de estos juguetes.
    - Guía de privacidad y seguridad en internet [11]: misma guía que la evaluada en el sitio web hermano Oficina de Seguridad del Internauta.
    - Guía de mediación parental [15]: tiene como objetivo el orientar a los padres somo como deben acompañar a sus hijos y cómo educarles en el uso seguro y responsable de Internet, dotándonos de estrategias, pautas y recomendaciones muy claras y entendibles que nos ayuden en este camino. Se trata de un recurso de gran calidad.
    - Catálogo de herramientas de control parental: ya comentado anteriormente.
    - Preguntas frecuentes
- Educadores: se centra en los recursos útiles en el entorno escolar, por lo que paso a enumerarlos, pero sin entrar a valorarlos en profundidad:
    - Artículos de ayuda para los responsables de TIC en los centros educativos.
    - Unidades didácticas para trabajar en el aula el uso seguro y responsable de Internet.
    - Guía de actuación en el centro educativo ante el ciberacoso.
    - Programa de cibercooperantes, mediante el que particulares con conocimientos de ciberseguridad dan charlas sensibilización en centros escolares.

Además de la clasificación mostrada anteriormente, existe una multitud de recursos interesantes a los que puede accederse mediante un buscador, tanto de contenido propio como de aquel publicado por otras entidades como puede ser las comunidades autónomas.

En resumen, un sitio muy recomendable y muy en línea con el propósito del presente TFM en aquellos hogares en los que haya menores, pero sin posibilidad de incorporación de una manera completa al mismo dado el gran volumen de información necesario para abarcar toda la casuística, por lo que la guía resultante tendría una extensión excesiva y no cumpliría el objetivo de sencillez.

Sí que debe mencionarse esta, e incorporar los elementos más importantes, pero dejando que los usuarios de la guía práctica de ciberseguridad en el hogar, resultante del presente TFM, accedan a la presente web para buscar información relevante para la edad y punto de madurez de sus hijos.

Vive Internet Seguro

La organización de consumidores y usuarios (OCU) junto con Google tienen la web "Vive un Internet seguro" [16] destinado a la ciberseguridad, donde se recoge una serie de medidas organizadas como un pequeño curso online sobre 6 aspectos básicos relacionados con la seguridad:

1. Conexión a Internet segura
2. Proteger los dispositivos
3. Proteger las cuentas personales
4. Cómo gestionar la privacidad en Internet
5. Compras en Internet
6. Niños e Internet

Los contenidos son muy claros y entendibles por todos los usuarios, y la usabilidad es muy buena, por lo que es un curso recomendable. En el lado negativo, hay temas que faltan (como las actualizaciones en otros dispositivos, minimizar superficie de ataque o el uso de autenticación multifactor) con lo que estimo que solamente trata un 50% de los problemas abordados por la presente guía y la profundidad de los contenidos es muy escasa por lo que solo van a ser útiles para aquellos usuarios sin ningún conocimiento de seguridad previo. Tomando ambos puntos en consideración, puede entenderse como un curso de concienciación e iniciación para los usuarios más inexpertos.

Otros recursos

Existen multitud de páginas web de ciberseguridad de diversas compañías, pero la mayoría de ellas tienen un contenido muy limitado, demasiado profundo o se trata de blogs en los que la frecuencia con la que aparecen los artículos no permite recomendarlos.

Entre estos sitios hay varios que conocía con anterioridad, y que nunca he encontrado con los contenidos, organización y claridad necesaria para poder recomendarlos a personas con bajos conocimientos informáticos.

Algunos ejemplos categorizados por la razón para descartarlos

1. Contenidos para usuarios demasiado avanzados / no siempre adecuados
    a. https://support.mozilla.org/es/products/privacy-and-security
    b. https://www.pandasecurity.com/spain/mediacenter/seguridad/
    c. https://www.adslzone.net/
    d. https://www.sans.org/security-resources/blogs
    e. https://www.t-systemsblog.es/tag/ciberseguridad/
2. Contenido poco actualizado
    a. https://www.bancosantander.es/es/particulares/banca-online/seguridad-online
    b. https://hacking-etico.com/
    c. https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

4.3. Conclusiones.

La Tabla 5 resume los sitios analizados, teniendo en cuenta los aspectos más relevantes para el presente TFM, según las definiciones recogidas en la Tabla 4.

Tabla 5. Aspectos principales de los sitios analizados
(Fuente: propia)

Criterio	Una al día	Oficina de Seguridad del Internauta	INTERNET SEGURA FOR KiDS	Vive Internet Seguro	Otros recursos
Usuarios objetivo	Expertos seguridad informática	Ciudadanos, hogares	Niños y adolescentes	Ciudadanos, hogares	Variable
Nivel mínimo usuarios	Medio	Bajo	Bajo	Bajo	Variable

Orientación	Incidentes de seguridad	Soporte e información de seguridad en Internet.	Uso seguro de Internet y nuevas tecnologías	Seguridad y privacidad en Internet	Variable
Objetivo	Divulgación	Educación	Educación	Educación	Variable
Completitud contenidos	Alto	Alto	Alto	Bajo	Variable
Claridad contenidos	Bajo	Alto	Alto	Alto	Variable
Organización contenidos	Medio	Alto	Alto	Alto	Variable
Contenidos actualizados	Alto	Alto	Alto	Bajo	Variable

En base a esta comparativa, recomiendo sugerir a los usuarios que empiecen por la página 'Vive un Internet seguro' y, una vez estén cómodos con todos los contenidos de la misma, pasen a profundizar conocimientos con la 'Oficina de Seguridad del Internauta' / 'Internet Segura 4 KiDS', navegando por las mismas en el orden que les parezca más adecuado para atajar primeros aquellos riesgos relacionados con aspectos que sean más relevantes para ellos o en los que se sientan más inseguros. Por último, una vez consideren que son capaces de entender la mayoría de los aspectos que se les presentan en dichas webs, deberían no tener miedo a la hora de buscar y acceder a contenidos relacionados con la seguridad en Internet, ya que de dispondrán de una base que les ayudará a juzgar la calidad (y utilidad) del contenido que descubran.

5. Objetivos

Como consecuencia de los resultados obtenidos en el estudio del estado del arte, recogidos en las Conclusiones., voy a pivotar levemente el objetivo del presente TFM de manera que voy a poner más foco en incorporar ciertos conocimientos que ya se encuentra disponible en dichos sitios web y menos en proporcionar una guía con menos contenido pero más visuales, dado que los dos principales problemas identificados son

- Desconocimiento de los recursos existentes para usuarios domésticos por parte de estos.
- Posible dificultad de los usuarios domésticos a la hora de abordar la ciberseguridad de sus hogares, dado la gran cantidad de información existente en las fuentes estudiadas sin una secuencia clara de aplicación, lo que puede tanto desanimar a los usuarios como conseguir que no pongan en práctica en primer lugar aquellas salvaguardas más relevantes.

5.1. Objetivo principal

El objetivo principal del presente TFM son

1. Generar una "Guía Práctica de Ciberseguridad en el Hogar", orientada a usuarios con pocos conocimientos informáticos que les permita proteger su hogar y a los miembros de la familia, con una ordenación de las distintas salvaguardas adecuada a los riesgos de los distintos recursos que pretenden proteger.

5.2. Sub-objetivos

A fin de poder cumplir el objetivo principal, se definen los siguientes objetivos parciales qué (una vez completados) permitirán abordar el mencionado objetivo

1. Identificar los principales activos a proteger.
2. Identificar las amenazas y hacer un análisis de riesgo de estas para seleccionar las que se van a abordar dentro de la guía.
3. Identificar las salvaguardas a introducir de cara a lograr mantener el nivel de riesgo por debajo del umbral seleccionado.
4. Buscar información en las fuentes identificadas, y en otras disponibles, para abordar la introducción de las salvaguardas en la guía.

5. Generar contenido asimilable por los usuarios, con indicaciones claras de los objetivos a conseguir y unas instrucciones precisas de cómo conseguirlo, o un enlace a instrucciones visuales para aquellas acciones más complejas.
6. Generar una “Guía práctica de Ciberseguridad en el Hogar”.

6. Metodología

La metodología que voy a emplear es la siguiente:

6.1 Análisis y gestión de riesgos

A la hora de identificar activos y seleccionar las salvaguardas a implementar para lograr una gestión adecuada de los riesgos voy a inspirarme en el marco Magerit.

Dado que el entorno doméstico no es el foco de dicho marco, será necesario adaptarse sobre la marcha y no tratar de asimilar la realidad del hogar a un entorno empresarial sino eliminar pasos y/o introducir elementos que no se contemplan en el mismo pero que son relevantes en este nuevo entorno.

La principal modificación viene derivada de tener en cuenta que en un hogar el activo más valioso son las personas que viven en él (a diferencia de una empresa donde lo son la información y los servicios que ofrece), por lo que la protección de estas personas ha sido el eje central del trabajo, y no unos activos secundarios como correspondería a una aplicación de Magerit en un entorno profesional.

6.2 Generación de la guía

Voy a agrupar las distintas amenazas en grupos relacionados y, para cada grupo, voy a tratar de introducir conjuntamente todas las medidas que los usuarios deben poner en práctica a fin de protegerse. Como una de las medidas más importantes, aunque transparente al usuario, cada uno de los grupos de amenazas contarán con unos apartados en los que se describe cual es la problemática y qué consecuencias puede tener si no se trata adecuadamente.

7. Análisis formal del riesgo

Para el análisis del riesgo con Magerit, voy a seguir los pasos enumerados en el estado del arte, en su apartado referido al ámbito empresarial. Aunque, como ya se ha indicado con anterioridad, sin seguirlo de manera precisa.

Los siguientes puntos recogen el análisis realizado.

7.1. Umbral de riesgo

A la hora de evaluar y gestionar el riesgo de una empresa, con anterioridad se realizan una serie de pasos entre los que se incluye la fijación del nivel de riesgo que es aceptable. En el caso que nos ocupa, voy a fijar dicho umbral en un nivel medio de riesgo, lo que implica que un hogar puede aceptar riesgos muy bajos, bajos o medios, pero que es necesario mitigar todo riesgo alto o muy alto que se identifique.

Esta aproximación es una simplificación de Magerit (y de cualquier aproximación profesional a la gestión de riesgos), en los que habitualmente se define un umbral por defecto de riesgo, pero se suele establecer un nivel de riesgo más estricto para ciertos activos, e incluso se puede relajar el riesgo aceptado para aquellos poco importantes.

En las empresas, los expertos en seguridad evalúan los activos y establecen cuales son los que hay que modificar dicho umbral por defecto, de manera que se puedan destinar los recursos de la manera más eficiente. Sin embargo, en un entorno doméstico no va a producirse esta adaptación del riesgo tolerado por activo, por lo que he decidido utilizar un umbral fijo para todos los activos, dado que el mismo activo debería tener umbrales distintos en distintos hogares (por ejemplo: una cámara de vigilancia WiFi vigilando una habitación en edificio de una ciudad y esa misma cámara apuntando a unas flores plantadas en un entorno rural).

Al no poder adaptarse el umbral a las condiciones particulares de cada activo en cada hogar, y por lo tanto las salvaguardas que de dicho valor se deriven, y dado el carácter de la guía para usuarios con pocos conocimientos (con lo que no se les debería proporcionar un exceso de medidas, o el resultado obtenido va a ser el abandono de la guía al considerarla fuera de su alcance), he optado por fijar dicho umbral fijo en el valor indicado a fin tratar de encontrar un equilibrio entre el riesgo residual y la cantidad y complejidad de las salvaguardas introducidas.

7.2. Obtención del catálogo de activos

Dado que la guía está orientada a usuarios sin experiencia, voy a centrarme en aquellos activos más relevantes y/o más comunes. Dentro de estos activos, voy a tratar tanto aquellos activos habituales en un sistema de información como aquellos relacionados con los miembros de la familia, como pudiera ser la privacidad y la educación de los menores.

Como se indica en Magerit, los activos esenciales de todo sistema de información son dos: la información que se maneja y los servicios que se prestan con dicho sistema. En el caso que nos ocupa, no es habitual que un entorno doméstico preste ningún servicio hacia el exterior, por lo que solamente voy a identificar los datos como activos esenciales a proteger, y los voy a agrupar como se muestra en la Tabla 6, en la que categorizo la información desde el punto de vista de los usuarios, y englobo dentro de cada una de las categorías tanto la información en sí como la protección de la privacidad, concienciación y protección de los usuarios en lo referente a cada uno de estos grupos. Así mismo, incluyo como esenciales a los miembros de las familias y en especial a los menores:

Tabla 6. Activos esenciales
(Fuente: propia)

Categoría	Activo	**Código Activo**	**Descripción**
Activos Esenciales: Información	Familiares	[AE.F]	Comprende todas las fotos, documentos, correos, facturas, etc. que pueden encontrarse tanto en formato digital como analógico, valorados como menos importantes por los usuarios. Cada usuario particular tendrá que decidir qué datos categoriza como 'familiares' y cuales como 'sensibles'.
	Sensible	[AE.S]	Subconjunto de la información familiar que es valorara como más importante por los usuarios desde el punto de vista de la privacidad o cualquier otro.

			Cada usuario particular tendrá que decidir qué datos categoriza como 'familiares' y cuales como 'sensibles'.
	Técnicos	[AE.T]	Tipo de datos normalmente ignorado por parte de los usuarios domésticos. Comprende aquellos datos de configuración necesarios para poder controlar su sistema, o para recuperarse de un desastre: datos de configuración (como la clave del sistema operativo), copias de los programas instalados que no puedan obtenerse de Internet, PIN y PUK del SIM de teléfono, etc.
	Identidad digital	[AE.ID]	Engloba toda la información que los miembros de una familia tienen en sus redes sociales, sus cuentas de correo, cuentas de los proveedores de servicio, etc. Dentro de esta identidad digital, un elemento a destacar son las credenciales (y claves criptográficas si las hubiera) que guarden los usuarios, y que por lo tanto son empleadas para identificarse ante los mencionados servicios.
	Exposición digital	[AE.ED]	Información relevante en el ámbito doméstico, aunque no pueda decirse que dicha información pertenezca a las familias. Comprende aquella parte de mundo digital a la que se ven expuestos los miembros de una familia: navegación en Internet, contenido de los videojuegos, correos recibidos, etc. Esta información puede ir desde en ambos sentidos: desde el hogar hacia Internet o desde Internet hacia el hogar.

Activos Esenciales: Personas	Integrantes del hogar	[AE.IH]	Todo miembro del hogar que debe ser protegido y educado.
	Menores en el hogar	[AE.MH]	Menores en el hogar que deben ser tutelados, protegidos y educados.

Respecto a los soportes más habituales en los que la información se encuentra almacenada, y se procesa, se puede destacar los siguientes activos recogidos en la Tabla 7:

Tabla 7. Activos soporte
(Fuente: propia)

Categoría	Activo	**Código Activo**	**Descripción**
Activos Soporte: HW, SW y media	Ordenador	[AS.O]	Ordenador personal, tanto portátil como de sobremesa, que hasta hace poco era el soporte fundamental, y por lo tanto la mayoría de los usuarios están más concienciados sobre la necesidad de protegerlo adecuadamente.
	Dispositivos móviles	[AS.DM]	Dispositivos que, sin llegar a ser un ordenador, manejan prácticamente la misma información, pero que se ven expuestos a una serie de riesgos bastante diferenciados. En este tipo de activos se puede destacar los teléfonos móviles y las tabletas.
	Papel	[AS.P]	En todo hogar queda una cantidad considerable de información en este formato bien de carácter puramente personal (por ejemplo, fotos) o más sensible (por ejemplo, la escritura de la vivienda). En este caso tendremos en cuenta aquellos documentos en papel que sean relevantes desde un punto de vista de ciberseguridad.

	Discos duros en la nube.	[AS.DDN]	Es habitual tanto que se usen para almacenar la información como copias de seguridad de esta. Ejemplos habituales pueden ser Dropbox, Google Drive, etc.
	Almacenamiento externo de información	[AS.AEI]	Soportes digitales móviles como pueden ser discos duros externos o llaves de memoria USB. Por su naturaleza, y por el uso diferenciado que hacemos de ellos, es habitual la pérdida o rotura de estos.

Hay una tercera categoría de activos, que son aquellos identificados como fundamentales para dar soporte al entorno digital doméstico más habitual, incluidos en la Tabla 8:

Tabla 8. Activos soporte digital
(Fuente: propia)

Categoría	Activo	**Código Activo**	**Descripción**
Redes de comunicaciones	Conexión a Internet	[RC.CI]	Engloba tanto a las conexiones cableadas cuando el usuario se encuentra en el hogar (fibra, ADSL) como el acceso a través de las redes de comunicaciones móviles en los dispositivos móviles y el acceso a través de WiFis públicas.
	Red comunicaciones doméstica	[RC.RCD]	Dentro del hogar, distribuye la conexión a Internet entre los distintos dispositivos, y permite la interconexión de los distintos dispositivos domésticos entre sí. Suele estar formada por el router del operador y una red WiFi doméstica.

Por último, aquellos dispositivos que no van a estar presentes en todos los hogares, pero que hacen aparición con cada vez más frecuencia en estos, mostrados en la Tabla 9:

Tabla 9. Activos auxiliares
(Fuente: propia)

Categoría	Activo	**Código Activo**	**Descripción**
Activos auxiliares	Periféricos	[AUX.P]	Dispositivos conectados directamente a los activos que dan soporte a la información: pulseras cuantificadoras, cámaras de videoconferencia, relojes inteligentes, etc.
	Otros dispositivos	[AUX.OD]	Dispositivos conectados a la red de datos. Hace tiempo que las consolas y los televisores disponen de conexión a Internet, pero cada vez es más frecuente que otros muchos dispositivos se conecten para poder recibir actualizaciones, para proporcionar información o ser controlables desde el exterior: lavadoras, luces inteligentes, neveras, …

En el presente trabajo, por limitación del tiempo disponible ante la amplia casuística existente, voy a centrarme únicamente en los tres primeros grupos de activos, y voy a realizar una simplificación consistente en no tratar cada uno de los activos individuales por separado (por ejemplo: fotos y facturas), sino que voy a realizar en análisis considerándolos en conjunto de acuerdo con las agrupaciones mostradas anteriormente (por ejemplo: información familiar).

Como parte de este paso de identificación de los activos, es necesario tanto aclarar las dependencias existentes entre ellos (en nuestro caso, los datos son dependientes del resto de activos, como se ha indicado anteriormente) como valorar la importancia de dichos activos, a fin de poder cuantificar (posteriormente) los riesgos a los que se ven expuestos.

En el análisis teórico a continuación, siguiendo la metodología Magerit, voy a excluir los 'Activos Esenciales: personas', por los siguientes motivos:

- El umbral de riesgo a tolerar no va a ser el mismo que en el resto de los activos, sino que se va a tratar todas las amenazas que se identifiquen.
- Muchas de las amenazas a estos activos en realidad son amenazas contra la información que tienen estas personas, y que por lo tanto van a identificarse y tratarse adecuadamente mediante el análisis de los activos de información.

- Su análisis queda más alejado de Magerit.

A la hora de valorar el resto de los activos, existen 5 dimensiones posibles, que son las características o atributos que hacen valiosos un activo, recogidas en la Tabla 10.

Tabla 10. Dimensiones de valoración
(Fuente: Magerit)

Dimensión	Definición
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
Integridad de los datos	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
Confidencialidad de la información	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

En el ámbito doméstico, considero que las más relevantes (y las únicas que voy a valorar) son la disponibilidad y la confidencialidad.

La integridad también es fundamental en este entorno, pero de manera general considero que las salvaguardas a introducir para garantizar la confidencialidad de las comunicaciones o la disponibilidad de los datos van a mitigar suficientemente los posibles problemas de integridad, con el añadido de que la mayoría de las medidas específicas que se puedan implantar para mitigar el riesgo de las amenazas específicas a la integridad van a quedar fuera de la capacidad técnica (o del presupuesto) de los usuarios objetivos, dado que las más sencillas ya están incorporadas directamente en el software empleado por los usuarios.

La trazabilidad y la autenticidad no las considero excesivamente relevantes en el presente ámbito de estudio, por la complejidad técnica de la implantación de las salvaguardas y la baja incidencia relativa de amenazas contra estas dos propiedades de seguridad, dado que las amenazas más comunes suelen acarrear la pérdida o acceso no autorizado a los datos, pero no la manipulación de estos.

El único caso en que la autenticidad es relevante se da en los intercambios de información con Internet (en general), que se incluyen dentro del activo 'Exposición Digital':

- a la hora de recibir información de un servicio (por ejemplo, un correo del banco) y poder detectar la autenticidad de este.
- a la hora de enviar información a un servicio (por ejemplo, realizar una transferencia) y poder asegurar que es el servicio legítimo.

Para el activo 'Exposición Digital' se va a incluir (entre otras) salvaguardas destinadas a mejorar la educación de los usuarios de cara a poder detectar los ataques de phishing o la legitimidad de un servidor como manera de mitigar estos dos casos.

Para las dimensiones a valorar, voy a asignar pesos para cada uno de los activos identificados, usando la tabla simplificada de valoración de Magerit, que es la adecuada para análisis de riesgo de poco detalle como el que estoy realizando. En dicha escala, cada activo debe valorarse en cada dimensión conforme a la Tabla 11.

Tabla 11. Criterio de valoración de los activos
(Fuente: Magerit)

Valor	Criterio
Extremo	Daño extremadamente grave
Muy Alto	Daño muy grave
Alto	Daño grave
Medio	Daño importante
Bajo	Daño menor
Despreciable	Irrelevante a efectos prácticos

Como parece lógico, la valoración de dichos activos va a basarse en mi punto de vista subjetivo, relacionado tanto con mi realidad familiar (2 hijos menores) como mí pasado (he experimentado la perdida de fotos y documentos digitales personales por rotura del disco duro donde se encontraba la única copia de estos archivos) o por mí forma de pensar, por lo que es perfectamente normal que existan discrepancias respecto a la misma según quién la realice. Mis valoraciones se incluyen en la Tabla 12.

Tabla 12. Valoración de los activos
(Fuente: propia)

Activo	**Disponibilidad**	**Confidencialidad**
[AE.F]	Alto	Medio
[AE.S]	Muy Alto	Alto
[AE.T]	Alto	Medio
[AE.ID]	Muy Alto	Muy Alto
[AE.ED]	Bajo	Alto
[AS.O]	Medio	Bajo
[AS.DM]	Alto	Alto
[AS.P]	Medio	Bajo
[AS.DDN]	Alto	Muy Alto
[AS.AE]	Bajo	Alto
[RC.CI]	Alto	Alto
[EC.RCD]	Medio	Alto

7.3. Identificación y análisis de las amenazas

En este punto voy a pensar no solo en aquellas amenazas externas, que son las que habitualmente reciben más atención y por lo tanto para las que hay más salvaguardas disponibles, sino también en todo aquello que puede poner en riesgo la disponibilidad o confidencialidad de los activos identificados, como podría ser quedarse sin datos en la conexión

a Internet del móvil porque al dejárselo a un menor dentro del hogar este ha deshabilitado sin querer la conexión WiFi y ha agotado los datos viendo dibujos.

Para el análisis de amenazas, analizo aquellas recogidas en el catálogo de amenazas de Magerit, según se muestra en la Tabla 13, en la que solamente incluyo aquellas amenazas relevantes.

Tabla 13. Análisis de amenazas
(Fuente: propia)

Categoría	**Amenaza**	**Análisis**
[N] Desastres naturales [I] De origen industrial	[N.1] Fuego [N.2] Agua [I.1] Fuego [I.2] Agua	En estos casos, se puede producir una pérdida total de los equipos informáticos, soportes de información y equipamiento auxiliar.
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	Esta amenaza es muy significativa dado el nivel de conocimientos de los usuarios, bajo y muy heterogéneo dentro de la misma unidad familiar.
	[E.8] Difusión de SW dañino	Los activos informáticos están expuestos a virus, programas espía, etc.
	[E.18] Destrucción de información	Los soportes informáticos están expuestos a fallos de funcionamiento. Todo soporte físico (analógico o digital) sufre un envejecimiento que conlleva la destrucción de la información que almacena.
	[E.19] Fugas de información	En el caso de los adultos es relevante, pero en los menores se debería asumir que van a hacer pública cualquier información que conozcan.
	[E.21] Errores de actualización de programas	Seguir utilizando versiones con defectos conocidos y reparados por el fabricante.

		Muchas veces viene ligado a la piratería, al no contar con soporte y por lo tanto no tener acceso a las nuevas versiones.
	[E.25] Pérdida de equipos	Es habitual la pérdida de los dispositivos móviles o de los almacenamientos externos de información.
[A] Ataques intencionados	[A.5] Suplantación de la identidad del usuario	Caben distinguir dos situaciones en las que se va a dar: - Atacante externo - Usuario interno no autorizado, como puede ser un menor.
	[A.11] Acceso no autorizado [A.18] Destrucción de la información. [A.19] Divulgación de información.	Acceso por parte de un atacante, principalmente por fallos en el sistema de identificación y autorización, a lo que puede seguir el resto de los casos. Puede darse tanto en los activos digitales como en los soportes físicos si no los tenemos protegidos adecuadamente.
	[A.25] Robo	Afecta a cualquier activo físico.
	[A.30] Ingeniería social	Afecta a los usuarios del sistema.

La Tabla 14 sintetiza, para cada activo, que amenazas son las que le afectan.

Tabla 14. Amenazas por activo
(Fuente: propia)

Activo	**Amenazas**
[AE.F]	[E.1], [E.18], [E.19], [A.11], [A.18], [A.19]
[AE.S]	[E.1], [E.18], [E.19], [A.11], [A.18], [A.19]

[AE.T]	[E.1], [E.18], [E.19], [A.11], [A.18], [A.19]
[AE.ID]	[E.1], [E.18], [E.19], [A.5], [A.11], [A.18], [A.19], [A.30]
[AE.ED]	[E.1], [E.18], [E.19], [A.5], [A.11], [A.18], [A.19], [A.30]
[AS.O]	[N.1], [N.2], [I.1], [I.2], [E.1], [E.8], [E.21], [E.25], [A.25]
[AS.DM]	[N.1], [N.2], [I.1], [I.2], [E.1], [E.8], [E.21], [E.25], [A.25]
[AS.P]	[N.1], [N.2], [I.1], [I.2], [E.1], [E.25], [A.25]
[AS.DDN]	[E.1], [E.18]
[AS.AE]	[N.1], [N.2], [I.1], [I.2], [E.1], [E.25], [A.25]
[RC.CI]	[E.1], [A.18], [A.19]
[RC.RCD]	[E.1], [E.21], [A.11], [A.18], [A.19]

En el caso de los activos relacionados con las personas, se identifican las siguientes amenazas, fuera del catálogo de Magerit y no incluidas ya en la “Tabla 14. Amenazas por activo”.

Tabla 15. Amenazas a miembros del hogar
(Fuente: propia)

Activo	Amenazas
[AE.IH]	Gestión inadecuada de la privacidad. Fraudes online
[AE.MH]	Exposición de los menores a dispositivos electrónicos e internet. Acceso a contenido inapropiado. Conexión con comunidades peligrosas. Ciberacoso Sexting

Como he comentado anteriormente, estas amenazas no van a ser analizadas formal y directamente van a proponerse medidas para mitigarlas.

7.4. Cálculo de impacto de las amenazas

Para valorar el impacto de las distintas amenazas, voy a valerme de la Tabla 16, que explica cómo se calcula el impacto de una amenaza a partir del valor del activo amenazado y de la degradación que la amenaza analiza causa en este activo. Por simplicidad, se eligen únicamente 3 posibles valores de degradación teniendo en cuenta el orden de magnitud de esta, y los resultados obtenidos se muestran en la Tabla 17.

Para cada activo, aun cuando se trata en realidad de un grupo de varios activos, no voy a tomar como valor de degradación el total de la degradación de los activos de dicho grupo (dado que una amenaza normalmente no degrada de una sola vez todos estos activos) sino el caso peor. Cuando, en apartados posteriores, trate de ver las salvaguardas a introducir, se tendrán en cuenta únicamente los activos individuales afectados.

Tabla 16. Estimación del impacto
(Fuente: Tema 4 – Sistemas de Gestión de la Seguridad [17])

impacto		***degradación***		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Un punto para destacar es que, la mayoría de los sistemas utilizados por los usuarios ya disponen de salvaguardas, y dichas salvaguardas han sido tenidas en cuenta a la hora de evaluar la degradación y el impacto de las amenazas en la Tabla 17. Cabe destacar, además, que la degradación se mide para un único incidente de seguridad, pero a la hora de valorarla no se tiene en cuenta todo el grupo de elementos incluidos dentro de cada activo sino el elemento más desfavorecido.

Tabla 17. Degradación e Impacto de las amenazas por activo
(Fuente: propia)

Activo	Valoración		Amenaza	Degradación		Impacto	
	Disp.	Conf.		Disp.	Conf.	Disp.	Conf.
[AE.F]	Alto	Medio	[E.1]	100%	100%	A	M
			[E.18]	100%	0%	A	MB
			[E.19]	0%	100%	MB	M
			[A.11], [A.18], [A.19]	100%	100%	A	M
[AE.S]	Muy Alto	Alto	[E.1]	100%	100%	MA	A
			[E.18]	100%	0%	MA	MB
			[E.19]	0%	100%	MB	A
			[A.11], [A.18], [A.19]	100%	100%	MA	A
[AE.T]	Alto	Medio	[E.1]	100%	10%	A	B
			[E.18]	100%	0%	A	MB
			[E.19]	0%	100%	MB	M
			[A.11], [A.18], [A.19]	100%	100%	A	M
[AE.ID]	Muy Alto	Muy Alto	[E.1]	100%	100%	MA	MA
			[E.18]	100%	0%	MA	MB
			[E.19]	0%	100%	MB	MA
			[A.11], [A.18], [A.19]	100%	100%	MA	MA
			[A.30]	10%	100%	A	MA
[AE.ED]	Bajo	Alto	[E.1]	10%	100%	MB	A
			[E.18]	100%	0%	B	MB

			[E.19]	0%	100%	MB	A
			[A.11], [A.18], [A.19]	100%	100%	B	A
			[A.30]	100%	100%	B	A
[AS.O]	Medio	Bajo	[N.1], [N.2], [I.1], [I.2]	100%	1%	M	MB
			[E.1]	100%	100%	M	B
			[E.8], [E.21], [E.25]	100%	100%	M	B
			[A.25]	100%	100%	M	B
[AS.DM]	Alto	Alto	[N.1], [N.2], [I.1], [I.2]	100%	1%	A	B
			[E.1]	100%	100%	A	A
			[E.8], [E.21], [E.25]	100%	100%	A	A
			[A.25]	100%	100%	A	A
[AS.P]	Medio	Bajo	[N.1], [N.2], [I.1], [I.2]	100%	1%	M	MB
			[E.1]	100%	100%	M	B
			[E.25]	100%	100%	M	B
			[A.25]	100%	100%	M	B
[AS.DDN]	Alto	Muy Alto	[E.1]	100%	10%	A	A
			[E.18]	100%	100%	A	MA
[AS.AE]	Bajo	Alto	[N.1], [N.2], [I.1], [I.2]	100%	1%	B	B
			[E.1]	100%	100%	B	A

			[E.25]	100%	100%	B	A
			[A.25]	100%	100%	B	A
[RC.CI]	Alto	Alto	[E.1]	100%	100%	A	A
			[A.11], [A.18], [A.19]	100%	100%	A	A
[EC.RCD]	Medio	Alto	[E.1]	100%	100%	M	A
			[E.21]	100%	100%	M	A
			[A.11], [A.18], [A.19]	100%	100%	M	A

7.5. Cálculo de la probabilidad de las amenazas

Para el cálculo de la probabilidad, voy a utilizar los 5 niveles tradicionales, mostrados en la Tabla 18.

Tabla 18. Niveles de probabilidad de una amenaza
(Fuente: Cálculo del riesgo – Tema 4 - Sistemas de Gestión de la Seguridad [18])

Valor	Símbolo	Criterio
Muy Alto	MA	Prácticamente seguro, muy frecuente, algo que puede ocurrir prácticamente a diario.
Alto	A	Probable, frecuente, algo que puede ocurrir mensualmente.
Medio	M	Posible, normal, una vez al año.
Bajo	B	Poco probable, poco frecuente, cada varios años.
Muy Bajo	MB	Muy raro, muy poco frecuente, algo que ocurre "una vez en la vida".

A la hora de calcular de las probabilidades de las distintas amenazas identificadas he tenido en cuenta las salvaguardas habituales existentes en los distintos servicios y programas utilizados por los usuarios. El resultado queda recogido en la Tabla 19.

Tabla 19. Cálculo de la probabilidad de las amenazas por activo
(Fuente: propia)

Activo	**Amenaza**	**Probabilidad**
[AE.F]	[E.1]	A
	[E.18]	M
	[E.19]	A
	[A.11], [A.18], [A.19]	M
[AE.S]	[E.1]	A
	[E.18]	M
	[E.19]	A
	[A.11], [A.18], [A.19]	M
[AE.T]	[E.1]	M
	[E.18]	M
	[E.19]	B
	[A.11], [A.18], [A.19]	B
[AE.ID]	[E.1]	A
	[E.18]	A
	[E.19]	A
	[A.11], [A.18], [A.19]	A
	[A.30]	MA
[AE.ED]	[E.1]	A
	[E.18]	A

	[E.19]	MA
	[A.11], [A.18], [A.19]	A
	[A.30]	MA
[AS.O]	[N.1], [N.2], [I.1], [I.2]	B
	[E.1]	A
	[E.8]	MA
	[E.21], [E.25]	A
	[A.25]	B
[AS.DM]	[N.1], [N.2], [I.1], [I.2]	B
	[E.1]	A
	[E.8]	MA
	[E.21], [E.25]	A
	[A.25]	M
[AS.P]	[N.1], [N.2], [I.1], [I.2]	B
	[E.1]	M
	[E.25]	M
	[A.25]	B
[AS.DDN]	[E.1]	M
	[E.18]	B
[AS.AE]	[N.1], [N.2], [I.1], [I.2]	B
	[E.1]	M
	[E.25]	A
	[A.25]	A
[RC.CI]	[E.1]	A

	[A.11], [A.18], [A.19]	MA
[RC.RCD]	[E.1]	A
	[E.21]	A
	[A.11], [A.18], [A.19]	A

7.6. Cálculo del riesgo

El cálculo del riesgo, una vez se conoce tanto el impacto como la probabilidad de una amenaza, se consigue utilizando la Tabla 20.

Tabla 20. Estimación del riesgo de una amenaza
(Fuente: Cálculo del riesgo – Tema 4 - Sistemas de Gestión de la Seguridad [18])

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Aplicando el cálculo visto en la Tabla 20 obtenemos finalmente la tabla del riesgo que supone cada amenaza identificada para cada una de las dimensiones evaluadas, para los distintos activos. El riesgo calculado se muestra en la Tabla 21.

Tabla 21. Riesgo de las amenazas por activo
(Fuente: propia)

Activo	**Amenaza**	**Impacto**		**Probabilidad**	**Riesgo**	
		Disp.	**Conf.**		**Disp.**	**Conf.**
[AE.F]	[E.1]	A	M	A	MA	A
	[E.18]	A	MB	M	A	MB
	[E.19]	MB	M	A	B	A

	[A.11], [A.18], [A.19]	A	M	M	A	M
[AE.S]	[E.1]	MA	A	A	MA	MA
	[E.18]	MA	MB	M	MA	MB
	[E.19]	MB	A	A	B	MA
	[A.11], [A.18], [A.19]	MA	A	M	MA	A
[AE.T]	[E.1]	A	B	M	A	B
	[E.18]	A	MB	M	A	MB
	[E.19]	MB	M	B	MB	M
	[A.11], [A.18], [A.19]	A	M	B	A	M
[AE.ID]	[E.1]	MA	MA	A	MA	MA
	[E.18]	MA	MB	A	MA	B
	[E.19]	MB	MA	A	B	MA
	[A.11], [A.18], [A.19]	MA	MA	A	MA	MA
	[A.30]	A	MA	MA	MA	MA
[AE.ED]	[E.1]	MB	A	A	B	MA
	[E.18]	B	MB	A	M	B
	[E.19]	MB	A	MA	B	MA
	[A.11], [A.18], [A.19]	B	A	A	M	MA
	[A.30]	B	A	MA	M	M
[AS.O]	[N.1], [N.2], [I.1], [I.2]	M	MB	B	M	MB

	[E.1]	M	B	A	A	M
	[E.8]	M	B	MA	A	M
	[E.21], [E.25]	M	B	A	A	M
	[A.25]	M	B	B	M	B
[AS.DM]	[N.1], [N.2], [I.1], [I.2]	A	B	B	A	B
	[E.1]	A	A	A	MA	MA
	[E.8]	A	A	MA	MA	MA
	[E.21], [E.25]	A	A	A	MA	MA
	[A.25]	A	A	M	A	A
[AS.P]	[N.1], [N.2], [I.1], [I.2]	M	MB	B	M	MB
	[E.1]	M	B	M	M	B
	[E.25]	M	B	M	M	B
	[A.25]	M	B	B	M	B
[AS.DDN]	[E.1]	A	A	M	A	A
	[E.18]	A	MA	B	A	MA
[AS.AE]	[N.1], [N.2], [I.1], [I.2]	B	B	B	B	B
	[E.1]	B	A	M	B	A
	[E.25]	B	A	A	M	MA
	[A.25]	B	A	A	M	MA
[RC.CI]	[E.1]	A	A	A	MA	MA
	[A.11], [A.18], [A.19]	A	A	MA	MA	MA

[EC.RCD]	[E.1]	M	A	A	A	MA
	[E.21]	M	A	A	A	MA
	[A.11], [A.18], [A.19]	M	A	A	A	MA

Como puede verse, hay multitud de amenazas que conllevan un riesgo superior al umbral 'Medio' que se ha establecido, lo que va a obligar a una adecuada gestión de estos.

8. Gestión del riesgo: selección contenidos a tratar en la guía

8.1. Limitaciones a las salvaguardas

A la hora de gestionar el riesgo, y elegir las salvaguardas a implementar, voy a estar fuertemente condicionado tanto por la dificultad que dichas medidas pudieran tener para un usuario inexperto como por el coste económico, puesto que la práctica totalidad de usuarios van a ser contrarios a realizar un gran desembolso de dinero y una amplia mayoría van a ser reluctantes ante cualquier gasto no justificado plenamente.

Ambos condicionantes van a limitar las posibles medidas y ser factores de peso a la hora de seleccionar cuando haya varias opciones disponibles.

Al mismo tiempo, el resto de las acciones posibles ante un riesgo (eliminar el activo o transferir el riesgo) voy a descartarlos dado que no es habitual que un usuario seleccione sus activos por criterios de seguridad (ej.: televisión sin conexión a internet frente a una que si lo tenga) ni que contrate seguros para hacer frente a los riesgos derivados de la exposición digital de los mismos.

8.2. Metodología

En este punto, veo conveniente apartarme ligeramente del método estrictamente formal que consistiría en una ordenación de los riesgos y la implantación sistemática de salvaguardas en ese orden, acudiendo al catálogo de Magerit.

En su lugar, voy a comenzar evaluando aquellas salvaguardas que son de más fácil implantación por parte de usuarios finales, y que sin duda son recomendaciones que deben estar en toda guía de ciberseguridad para usuarios finales. A continuación, volveré a evaluar los riesgos residuales para (entonces sí) pasar a tratar aquellos riesgos que no hayan sido mitigados adecuadamente.

El resultado obtenido debería ser análogo al uso habitual de Magerit, pero evitará que se incluya alguna medida de difícil implantación cuando varias medidas sencillas son capaces de mitigar el riesgo adecuadamente.

Una vez estén identificadas todas las salvaguardas a implementar se procederá a seleccionar y desarrollar los textos detallados a presentar a los usuarios.

8.3. Salvaguardas iniciales

Las áreas más repetidas tanto en los sitios incluidos en el estado del arte como en otros consultados son las incluidas en los siguientes subapartados.

Cómo se ha indicado anteriormente, se ha tratado de hacer una selección de un número limitado de áreas y de salvaguardas para quedarnos con aquellas que conjuguen una utilidad manifiesta junto con una sencillez de cara a la puesta en práctica por usuarios no expertos.

Para cada área se van a sugerir las salvaguardas más habituales, pero no se va a profundizar en su contenido dado que eso será objeto de apartados posteriores.

8.3.1. Uso de software actualizado

Este punto que es tan conocido en el mundo empresarial, lo cual no quiere decir que todas las empresas lo implementen adecuadamente, no es en absoluto tan conocido en el entorno doméstico. Es perfectamente habitual encontrarse con una o varias de las siguientes situaciones:

- Dispositivos (principalmente router) con un firmware desactualizado, y con vulnerabilidades graves conocidas.
- Uso de software pirata, lo que conlleva que no se pueda instalar los parches del fabricante, dado que se depende de la última versión que se haya conseguido piratear, lo que implica que la versión instalada tenga vulnerabilidades conocidas.
- Instalación de software desde fuentes de dudosa reputación, por lo que puede implicar que dicho software venga contaminado con algún tipo de malware. Esto puede darse tanto en el caso de instalar una versión pirateada como cuando (aparentemente) estamos intentando instalar el programa original, pero desde una fuente no oficial.
- Desconocimiento por parte de los usuarios de las implicaciones que conlleva el uso de software con vulnerabilidades, por lo que muchas veces no existe un interés por su parte de conseguir actualizarlo o directamente se rechaza la búsqueda e instalación automática de actualizaciones.

A la vista de los problemas descritos, las salvaguardas que se pueden proponer en este apartado serían las siguientes

1. Instalación de software legal desde las fuentes oficiales, con indicaciones para Windows, iOS y Android.

2. Habilitar las actualizaciones automáticas, y aceptar las actualizaciones que nos ofrezcan, con indicaciones para Windows, iOS y Android.
3. Revisión periódica de la existencia de actualizaciones de seguridad en aquellos dispositivos que no realicen la búsqueda de actualizaciones de manera automática, como pueden ser las televisiones y los routers, y en los que normalmente deberemos conectarnos a la página web de soporte del fabricante del mismo e introducir nuestro número de modelo a fin de poder bajarnos la última versión disponible, que deberemos instalar a continuación desde alguna opción del menú de administración del dispositivo.
4. Educación de los usuarios respecto a la problemática descrita anteriormente.

8.3.2. Minimizar la superficie de ataque

Este punto es bastante complejo de transmitir a los usuarios finales, dada la gran casuística de entornos y necesidades distintas, por lo que las salvaguardas que se van a proponer son por naturaleza incompleta, centradas en aquellos dispositivos más habituales:

5. Desinstalar aquellos programas que hayan dejado de utilizar.
6. Ordenadores Windows
   6.1. Conseguir que el centro de seguridad indique todo está correcto.
   6.2. Minimizar las extensiones instaladas en el navegador.
7. Dispositivos Android: fortalecimiento básico.
8. Dispositivos iOS: fortalecimiento básico.
9. Router y conexión WiFi: fortalecimiento básico.
10. Educar a los usuarios sobre la importancia de minimizar la superficie de ataque.

8.3.3. Realizar copias de seguridad

Muchos de los riesgos identificados conllevaban una pérdida de los datos, dado que es bastante común que los usuarios no dispongan de copias de seguridad de los datos, o que el sistema de copias de seguridad sea ineficiente e ineficaz y consista en la realización de copias de parte de los datos en el propio dispositivo o en un disco duro externo (o dispositivo USB) que puede verse afectados por el mismo incidente que conlleve la pérdida del medio de almacenamiento original.

Las salvaguardas que propongo en este apartado son las siguientes:

11. Implantar un sistema de copias de seguridad adecuado

11.1. Hay que identificar qué datos son más importantes, de cara a aumentar la redundancia. En nuestro caso, son los [AE.S], [AE.T] y [AE.ID].

11.2. Para los datos más importantes, es necesario disponer de dos copias de seguridad de estos: una local en un dispositivo extraíble y una segunda copia en la nube. Nota: La copia local para dispositivos móviles puede no estar al alcance (técnico) de todos los usuarios, por lo que se sugerirá la copia en 2 nubes distintas.

11.3. Los datos menos importantes pueden disponer únicamente de copia de seguridad local.

11.4. Aquellos datos relevantes para los que solo exista copia en papel deben digitalizarse.

12. Recomendaciones sobre los distintos servicios en la nube que existen, configuración segura y como conseguir realizar la copia desde Windows, Android e iOS.

8.3.4. Protección de la identidad digital

Los problemas más comunes que se dan en este ámbito son los siguientes

- Uso de contraseñas inseguras.
- Reutilización de contraseñas.
- Almacenamiento inseguro de contraseñas.
- No activación de la autenticación multifactor.

En este caso las salvaguardas a sugerir son las siguientes

13. Uso de un gestor de contraseñas
    13.1. Para la generación de contraseñas
    13.2. Para el almacenamiento de las contraseñas
14. Activación de la autenticación multifactor.
15. Almacenamiento seguro del fichero de contraseñas.
16. Educación sobre la protección de la identidad digital.

8.3.5. Educación de los usuarios

La educación de los usuarios se ha ido atacando dentro de cada uno de los puntos anteriores, y la guía incluirá todos aquellos contenidos interesantes (y de fácil entendimiento) que haya encontrado. Adicionalmente, como se ha indicado anteriormente, se van a introducir aquellas

salvaguardas que, mediante la educación de los usuarios, mitiguen los riesgos derivados de las amenazas que se recogen en la "Tabla 15. Amenazas a miembros del hogar"

17. Educación sobre comercio electrónico
18. Educación sobre la gestión de la privacidad en Internet
19. Educación sobre conexión a Internet segura
20. Educación sobre los menores e Internet

8.4. Evaluación de las salvaguardas iniciales

Una vez identificadas las salvaguardas a introducir, es necesario evaluar como dichas medidas afectan a la probabilidad de que las amenazas se materialicen o a la degradación que producen, a fin de evaluar el riesgo residual.

Para ello, amenaza a amenaza, hay que evaluar cuales de las medidas propuestas en "Salvaguardas iniciales" son relevantes. Una salvaguarda es relevante para una amenaza cuando afecta a la valoración de esta en las dimensiones de degradación o de probabilidad, y su contribución se expresa como el porcentaje de disminución de la probabilidad de ocurrencia o como el porcentaje de disminución de la degradación, según la dimensión.

Si múltiples salvaguardas afectas a la misma dimensión de un activo, puede optarse por utilizarse el porcentaje de reducción mayor o por realizar un cálculo combinado teniendo en cuenta todas las salvaguardas en conjunto. En el presente TFM, voy a optar por realizar una valoración conjunta de todas las salvaguardas que mitiguen una amenaza, dado que va a ser necesario una implementación sencilla de las salvaguardas con lo que la efectividad de cada salvaguarda de manera aislada no va a ser tan elevada como cuando se implementa en un entorno más profesional.

Una vez calculados, se aplica de nuevo la "Tabla 20. Estimación del riesgo de una amenaza" pero utilizando como valores de degradación y probabilidad aquellos resultantes de tener en cuenta las salvaguardas relevantes, según recoge la Tabla 22. En dicha tabla, la columna de las salvaguardas indica (para cada una de las 3 dimensiones a estudiar: cómo afecta al impacto en la disponibilidad, como afecta al impacto en la confidencialidad y como afecta a la probabilidad) se incluyen la lista de salvaguardas identificadas (referenciadas por los números 1 a 20, según se han propuesto anteriormente) y el porcentaje estimado de cómo afectan a la dimensión bajo estudio.

Tabla 22. Riesgo residual de las amenazas por activo
(Fuente: propia)

Activo	Amenaza	Degradación		Prob.	Riesgo		Salvaguardas y disminución degradación / probabilidad			Impacto Residual		Prob. Res.	Riesgo Residual	
		Disp.	Conf.		Disp.	Conf.	Degradación Disponibilidad	Degradación Confidenc.	Prob.	Disp.	Conf.		Disp.	Conf.
[AE.F] Disp: A Conf: M	[E.1]	100%	100%	A	MA	A	11, 12: -90%	16, 18, 19, 20: -90%	16, 18, 19, 20: -80%	M	B	M	M	B
	[E.18]	100%	0%	M	A	MB	11, 12: -90%	-	16, 18, 19, 20: -80%	M	MB	B	M	MB
	[E.19]	0%	100%	A	B	A	-	16, 18, 19, 20: -90%	16, 18, 19, 20: -80%	MB	B	M	MB	B
	[A.11], [A.18], [A.19]	100%	100%	M	A	M	11, 12: -90%	1 a 10, 16 a 20: -90%	1 a 10, 16 a 20: -90%	M	B	B	M	B
[AE.S] Disp: MA Conf: A	[E.1]	100%	100%	A	MA	MA	11, 12: -99%	16, 18, 19, 20: -90%	16, 18, 19, 20: -80%	M	M	M	M	M
	[E.18]	100%	0%	M	MA	MB	11, 12: -99%	-	16, 18, 19, 20: -80%	M	MB	B	M	MB
	[E.19]	0%	100%	A	B	MA	-	16, 18, 19, 20: -90%	16, 18, 19, 20: -80%	MB	M	M	MB	M
	[A.11], [A.18], [A.19]	100%	100%	M	MA	A	11, 12: -99%	1 a 10, 16 a 20: -90%	1 a 10, 16 a 20: -90%	M	M	B	M	M
[AE.T] Disp: A Conf: M	[E.1]	100%	10%	M	A	B	11, 12: -99%	16, 18, 19, 20: -90%	16, 18, 19, 20: -80%	B	MB	B	B	MB
	[E.18]	100%	0%	M	A	MB	11, 12: -99%	-	16, 18, 19, 20: -80%	B	MB	B	B	MB
	[E.19]	0%	100%	B	MB	M	-	16, 18, 19, 20: -90%	16, 18, 19, 20: -80%	MB	MB	MB	MB	MB
	[A.11], [A.18], [A.19]	100%	100%	B	A	M	11, 12: -99%	1 a 10, 16 a 20: -90%	1 a 10, 16 a 20: -90%	B	B	MB	MB	MB
[AE.ID] Disp: MA Conf: MA	[E.1]	100%	100%	A	MA	MA	11, 12, 13, 15: -99%	13, 15, 16, 17, 18, 19, 20: -99%	13, 15, 16, 17, 18, 19, 20: -90%	M	M	M	M	M
	[E.18]	100%	0%	A	MA	B	11, 12, 13, 15: -99%	-	13, 15, 16, 17, 18, 19, 20: -90%	M	MB	M	M	MB

	[E.19]	0%	100%	A	B	MA	-	13, 15, 16, 17, 18, 19, 20: -99%	13, 15, 16, 17, 18, 19, 20: -90%	MB	M	M	MB	M
	[A.11], [A.18], [A.19]	100%	100%	A	MA	MA	11, 12, 13, 15: -99%	1 a 10, 13 a 20: -99%	1 a 10, 13 a 20: -99%	M	M	B	M	M
	[A.30]	10%	100%	MA	MA	MA	11, 12, 13, 15: -99%	1 a 10, 13 a 20: -99%	1 a 10, 13 a 20: -99%	M	M	M	M	M
[AE.ED] Disp: B Conf: A	[E.1]	10%	100%	A	B	MA	11, 12: -90%	4, 10, 16, 17, 18, 19, 20: -90%	4, 10, 16, 17, 18, 19, 20: -90%	MB	M	M	MB	M
	[E.18]	100%	0%	A	M	B	11, 12: -90%	-	4, 10, 16, 17, 18, 19, 20: -90%	MB	MB	M	MB	MB
	[E.19]	0%	100%	MA	B	MA	-	4, 10, 16, 17, 18, 19, 20: -90%	4, 10, 16, 17, 18, 19, 20: -90%	MB	M	A	B	A
	[A.11], [A.18], [A.19]	100%	100%	A	M	MA	11, 12: -90%	1 a 10, 16 a 20: -90%	1 a 10, 16 a 20: -90%	MB	M	M	MB	M
	[A.30]	100%	100%	MA	M	M	11, 12: -90%	1 a 10, 16 a 20: -90%	1 a 10, 16 a 20: -90%	MB	M	A	MB	A
[AS.O] Disp: M Conf: B	[N.1], [N.2], [I.1], [I.2]	100%	1%	B	M	MB	11, 12: -50%	-	-	M	MB	B	M	MB
	[E.1]	100%	100%	A	A	M	1, 2, 4, 6, 10, 11, 12: -90%	1, 2, 4, 6, 10, 16 a 20: -90%	1, 2, 4, 6, 10, 16 a 20: -90%	B	MB	B	B	MB
	[E.8]	100%	100%	MA	A	M	1, 2, 4, 5, 6, 10, 11, 12: -90%	1, 2, 4, 5, 6, 10, 17 a 20: -90%	1, 2, 4, 5, 6, 10, 17 a 20: -90%	B	MB	A	M	B
	[E.21], [E.25]	100%	100%	A	A	M	1, 2, 4, 5, 6, 10, 11, 12: -90%	1, 2, 4, 5, 6, 10, 17 a 20: -90%	1, 2, 4, 5, 6, 10, 17 a 20: -90%	B	MB	M	B	MB
	[A.25]	100%	100%	B	M	B	-	-	-	M	B	B	M	B

[AS.DM] Disp: A Conf: A	[N.1], [N.2], [I.1], [I.2]	100%	1%	B	A	B	11, 12: -90%	-	-	M	B	B	M	B
	[E.1]	100%	100%	A	MA	MA	1, 2, 4, 7, 8, 10, 11, 12: -90%	1, 2, 4, 7, 8, 10, 16 a 20: -90%	1, 2, 4, 7, 8, 10, 16 a 20: -90%	M	M	M	M	M
	[E.8]	100%	100%	MA	MA	MA	1, 2, 4, 5, 7, 8, 10, 11, 12: -90%	1, 2, 4, 5, 7, 8, 10, 17 a 20: -90%	1, 2, 4, 5, 7, 8, 10, 17 a 20: -99%	M	M	M	M	M
	[E.21], [E.25]	100%	100%	A	MA	MA	1, 2, 4, 5, 7, 8, 10, 11, 12: -90%	1, 2, 4, 5, 7, 8, 10, 17 a 20: -90%	1, 2, 4, 5, 7, 8, 10, 17 a 20: -99%	M	M	B	M	M
	[A.25]	100%	100%	M	A	A	11, 12: -90%	-	-	M	A	M	M	A
[AS.P] Disp: M Conf: B	[N.1], [N.2], [I.1], [I.2]	100%	1%	B	M	MB	11, 12: -99%	-	-	MB	MB	B	MB	MB
	[E.1]	100%	100%	M	M	B	11, 12: -99%	-	-	MB	B	B	MB	B
	[E.25]	100%	100%	M	M	B	11, 12: -99%	-	-	MB	B	B	MB	B
	[A.25]	100%	100%	B	M	B	-	-	-	M	B	B	B	B
[AS.DDN]	[E.1]	100%	10%	M	A	A	11, 12: -90%	12: -90%	12: -90%	M	M	B	M	M
Disp: A Conf: MA	[E.18]	100%	100%	B	A	MA	11, 12: -90%	12: -90%	12: -90%	M	A	MB	B	M
[AS.AE] Disp: B Conf: A	[N.1], [N.2], [I.1], [I.2]	100%	1%	B	B	B	11, 12: 0%	-	-	B	B	B	B	B
	[E.1]	100%	100%	M	B	A	11, 12: -90%	-	-	MB	A	M	MB	A
	[E.25]	100%	100%	A	M	MA	11, 12: -90%	-	-	MB	A	A	B	MA
	[A.25]	100%	100%	A	M	MA	-	-	-	B	A	A	M	MA
[RC.CI]	[E.1]	100%	100%	A	MA	MA	19: -90%	19: -90%	19: -90%	M	M	M	M	M
Disp: A Conf: A	[A.11], [A.18], [A.19]	100%	100%	MA	MA	MA	19: -90%	19: -90%	19: -90%	M	M	M	M	M

[EC.RCD] Disp: M Conf: A	[E.1]	100%	100%	A	A	MA	9, 10, 16-19: -90%	9, 10, 16-19: -90%	9, 10, 16-19: -90%	B	M	M	B	M
	[E.21]	100%	100%	A	A	MA	2, 3, 4, 9, 10: -90%	2, 3, 4, 9, 10: -90%	2, 3, 4, 9, 10: -90%	B	M	M	B	M
	[A.11], [A.18], [A.19]	100%	100%	A	A	MA	2, 3, 4, 9, 10: -90%	2, 3, 4, 9, 10: -90%	2, 3, 4, 9, 10: -90%	B	M	M	B	M

8.5. Salvaguardas adicionales

A la vista de los resultados obtenidos en la Tabla 22, quedan 6 amenazas que conducen a un riesgo superior al umbral seleccionado, y que quedan recogidas en la Tabla 23.

Tabla 23. Amenazas con riesgo residual por encima del umbral seleccionado (Fuente: propia)

Activo	Amenaza	Degradación		Prob.	Riesgo		Salvaguardas y disminución degradación / probabilidad			Impacto Residual		Prob. Res.	Riesgo Residual	
		Disp.	Conf.		Disp.	Conf.	Degradación Disponibilidad	Degradación Confidenc.	Prob.	Disp.	Conf.		Disp.	Conf.
[AE.ED] Disp: B Conf: A	[E.19]	0%	100%	MA	B	MA	-	4, 10, 16, 17, 18, 19, 20: -90%	4, 10, 16, 17, 18, 19, 20: -90%	MB	M	A	B	A
	[A.30]	100%	100%	MA	M	M	11, 12: -90%	1 a 10, 16 a 20: -90%	1 a 10, 16 a 20: -90%	MB	M	A	MB	A
[AS.DM] Disp: A Conf: A	[A.25]	100%	100%	M	A	A	11, 12: -90%	-	-	M	A	M	M	A
[AS.AE] Disp: B Conf: A	[E.1]	100%	100%	M	B	A	11, 12: -90%	-	-	B	A	M	B	A
	[E.25]	100%	100%	A	M	MA	11, 12: -90%	-	-	MB	A	A	B	MA
	[A.25]	100%	100%	A	M	MA	-	-	-	B	A	A	M	MA

Un análisis conjunto de las 6 amenazas y sus consecuencias muestra que en realidad tenemos los siguientes grupos:

- Divulgación (voluntaria o involuntaria) de información
    - [AE.ED] – [E.19]
    - [AE.ED] – [A.30]
- Acceso a la información tras la pérdida o robo de un dispositivo
    - [AS.DM] – [A.25]
    - [AS.AE] – [E.25]
    - [AS.AE] – [A.25]
- Errores en la manipulación de un dispositivo externo (memoria USB, disco duro externo) exponen su información
    - [AS.AE] – [E.1]

Las nuevas salvaguardas para mitigar esas amenazas son

21. Evitar acceso a la información sensible / importante a los menores.
22. Evitar el almacenamiento de información sensible / importante en dispositivos móviles y almacenamientos externos.
23. Uso de mecanismos de autenticación, autorización y cifrado en dispositivos móviles y almacenamiento externo.

El análisis del impacto de dichas salvaguardas adicionales se recoge en la Tabla 24.

Tabla 24. Análisis salvaguardas adicionales
(Fuente: propia)

Activo	Amenaza	Degradación		Prob.	Riesgo		Salvaguardas y disminución degradación / probabilidad			Impacto Residual		Prob. Res.	Riesgo Residual	
		Disp.	Conf.		Disp.	Conf.	Degradación Disponibilidad	Degradación Confidenc.	Prob.	Disp.	Conf.		Disp.	Conf.
[AE.ED] Disp: B Conf: A	[E.19]	0%	100%	MA	B	MA	-	4, 10, 16, 17, 18, 19, 20, 21: -99%	4, 10, 16, 17, 18, 19, 20, 21: -99%	MB	B	M	MB	B
	[A.30]	100%	100%	MA	M	M	11, 12: -90%	1 a 10, 16 a 21: -99%	1 a 10, 16 a 21: -99%	MB	B	M	MB	B
[AS.DM] Disp: A Conf: A	[A.25]	100%	100%	M	A	A	11, 12: -90%	22, 23: -99%	-	M	A	MB	B	M

[AS.AE] Disp: B Conf: A	[E.1]	100%	100%	M	B	A	11, 12: -90%	22, 23: -90%	22, 23: -50%	MB	M	M	MB	M
	[E.25]	100%	100%	A	M	MA	11, 12: -90%	22, 23: -99%	-	MB	B	A	B	M
	[A.25]	100%	100%	A	M	MA	-	22, 23: -99%	-	B	B	A	M	M

11. Desarrollo guía

Para desarrollar la guía, voy a generar una tarjeta por cada uno de los temas, y en dicha tarjeta trataré de incluir el siguiente contenido, poniendo especial énfasis en el uso de un lenguaje sencillo de entender y con explicaciones cortas, enlazando con aquellos contenidos online que puedan explicar más en detalle cada punto:

1. Breve explicación de la problemática.
2. Problemas frecuentes de seguridad, y sus consecuencias.
3. Medidas de protección básicas
4. Comprobación rápida
5. Recursos para aprender más.

Así mismo, generaré una tarjeta adicional para el conjunto de la guía.

A continuación, expongo el texto a incluir en cada uno de los apartados de las distintas tarjetas.

11.1. Tarjeta introducción

11.1.1. Introducción

Internet se ha convertido en un elemento esencial de nuestras vidas, a través del cual accedemos a multitud de servicios (banca, compras, medios de comunicación, etc.) y ocio (videojuegos, música, películas y series), y cada vez más es un medio en el que nos relacionamos unos con otros (redes sociales, compartición fotos y videos, etc.).

Todo lo anterior conlleva que nuestros datos personales e información privada viaja por la red de redes y debemos ser conscientes de los riesgos a los que nos exponemos y aquellas medidas que nos permitan mejorar nuestra seguridad y mantener un nivel de privacidad adecuado.

11.1.2. Contenido

Esta “Guía Práctica de Ciberseguridad en el Hogar” trata de abordar la tarea de proteger los distintos aspectos relacionados con la ciberseguridad en el hogar, orientándose a aquellos usuarios con menos conocimientos en la materia.

Las siguientes tarjetas van a centrarse en cada uno de estos aspectos, tratando de identificar de una manera sencilla los peligros más habituales y como protegernos ante ellos. Las distintas tarjetas se pueden ir aplicando en el orden que sea más conveniente o sencillo a cada uno.

Para aquellos usuarios que ya hayan puesto en práctica todas las medidas elementales incluidas en las fichas, se añade un apartado donde es posible conseguir información para profundizar más.

11.1.3. Medidas de protección básicas

A modo introductorio es conveniente comenzar por seguir el breve curso "*Vive un Internet Seguro*", creado conjuntamente por Google y la OCU y que incluye información sobre los siguientes puntos:

1. Conexión a Internet segura
2. Proteger los dispositivos
3. Proteger las cuentas personales
4. Cómo gestionar la privacidad en Internet
5. Compras en Internet
6. Niños e Internet

11.1.4. Comprobación rápida

En este apartado, de cada tarjeta, se incluirán unos puntos para poder auto-diagnosticar el estado actual respecto a los puntos explicados en la misma, de manera que cada persona pueda ajustar el orden de lectura e implementación de las medidas de protección para atacar primero aquellos aspectos en los que sea más vulnerable.

11.1.5. Recursos para aprender más

Si bien existen multitud de páginas web, las más recomendables para los usuarios domésticos son las siguientes:

- Oficina de Seguridad del Internauta, del Instituto Nacional de Ciberseguridad (INCIBE): https://www.osi.es/es. Si se desea recibir las alertas de seguridad que nos mantengan al día de los nuevos problemas de seguridad que puedan afectarnos, es recomendable subscribirse a los avisos de ducha página: https://www.osi.es/es/actualidad/avisos.

- Internet Segura 4 KiDS, del Instituto Nacional de Ciberseguridad, enfocada en la protección y educación de los menores: https://www.is4k.es/.
- Centro criptológico nacional: https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad.html. Es conveniente destacar las guías especializadas sobre los distintos aspectos de la seguridad, donde es posible encontrar información completa y fiable.

En cualquier caso, es posible encontrar información detallada sobre cualquier tema utilizando un buscador, pero es recomendable hacerlo una vez ser haya adquirido ciertos conocimientos para aprender a discernir la calidad y validez de lo que se encuentre.

11.2. Evitar la pérdida de los datos

11.2.1. Explicación problemática

Cada vez tenemos más datos digitales que tienen cierto valor personal, o cuya pérdida podría tener consecuencias económicas, pero muchas veces confiamos su almacenamiento a un único dispositivo y asumimos que va a seguir allí cuando pudiéramos necesitarla de nuevo.

Sin embargo, la realidad nos demuestra que hay muchas ocasiones en las que no encontramos un dato o archivo que queremos recuperar, por lo que es necesario poner en marcha un sistema efectivo y eficaz de copias de seguridad para asegurar la disponibilidad de todo aquello que queremos conservar.

11.2.2. Problemas frecuentes de seguridad y sus consecuencias

Varias de las situaciones más habituales que conllevan una pérdida de los datos son las siguientes:

- El medio donde se encuentra el dato o archivo (disco duro, teléfono, llave USB, etc.) deja de estar accesible por pérdida, robo o por simple rotura.
- El medio donde se encuentra el dato o archivo se encuentra protegido por una contraseña, y al olvidarnos de la misma dejamos de poder tener acceso a su contenido.
- Un error del usuario durante el manejo del medio de almacenamiento provoca que se borre su contenido.
- Un virus infecta el ordenador o teléfono, haciéndonos perder todo su contenido.

11.2.3. Medidas de protección básicas

La medida más importante para prevenir la pérdida de datos es la implantación de un sistema de copias de seguridad, de tal manera que se asegure que se pueda recuperar el mismo a partir de su copia si existiera algún problema con el original.

Para que dicho sistema de copias de seguridad sea efectivo y eficaz, debe tener en cuenta los siguientes puntos:

- Aquellos datos más importantes deben disponer de dos copias de seguridad en ubicaciones distintas, a fin de que podamos recuperarlo aún en el improbable caso de que fallen simultáneamente el original y una de las copias de seguridad. Un archivo muy importante es aquel en el que el gestor de contraseñas almacena todas las contraseñas.
- Para poder reducir el coste de las copias de seguridad, los datos menos importantes pueden disponer de una única copia de seguridad.
- Existen dos tipos de copias de seguridad
    - Copias de seguridad locales: copias que se realizan en un disco duro externo, DVD o un ordenador.
    - Copias de seguridad en la nube: Copias realizadas en un servicio en la nube como Microsoft OneDrive, Google Drive, Dropbox, etc.
- Protege las copias de seguridad de acuerdo con los datos que contengan, por lo que será necesario cifrar las copias de seguridad locales / configurar adecuadamente los mecanismos de seguridad en los servicios en la nube para asegurarnos que los datos solamente sean accesibles por nosotros.
- Como norma general, evita almacenar información sensible en dispositivos móviles y almacenamientos externos (discos duros externos, llaves USB) dado que son propensos a ser robados o perdidos. Caso de que necesites hacerlo, asegúrate que lo proteges adecuadamente mediante cifrado.
- Si algún dato relevante está en papel, se puede hacer una foto al mismo para convertirlo en un archivo digital.
- No te olvides de aquellos datos necesarios para restaurar tu ordenador / teléfono / tableta: licencias de los programas, instaladores e instrucciones de instalación, etc.
- Las copias de seguridad deben realizarse de manera periódica, no basta con realizar una copia de seguridad en un momento determinado y olvidarse. Es por ello que es más cómodo el realizar las copias en la nube de manera automática.

- Es importante comprobar periódicamente el acceso a las copias de seguridad, así como determinar que se están haciendo adecuadamente y que somos capaces de recuperar el contenido.
- Hay que asegurarse que los servicios de almacenamiento en la nube se configuran adecuadamente, de manera que todos los archivos que subamos sean accesibles únicamente por nosotros. Para aprender a configurarlo de esta manera, es necesario leerse los manuales de ayuda del servicio seleccionado.
- Si se quiere compartir algún documento almacenado en un servicio en la nube con terceras personas es necesario determinar si el permiso que se quiere dar a dicha persona es de solo-lectura o de lectura-escritura. Para configurarlo, hay que leer la documentación de dicho servicio a fin de asegurarnos que hemos configurado la compartición de manera adecuada.

Nota: la protección contra virus, gestión de contraseñas y demás situaciones descritas en el apartado de problemas frecuentes se abordan en otros apartados de la guía.

11.2.4. Comprobación rápida

Esta área se encuentra adecuadamente protegida si:

- Tienes clasificados los archivos digitales y conoces donde almacenas todos aquellos que consideras más importantes, tanto por contener información sensible como por su valor sentimental.
- Tienes copia de seguridad de todos los archivos suficientemente importantes, y verificas periódicamente que siga funcionando.
- Tienes dos copias de seguridad de los archivos más importantes, y están protegidas por contraseña.
- Sabes cómo recuperar todo el contenido de tus dispositivos (ordenador, teléfonos, etc.) a partir de estas copias de seguridad, caso de que dejen de funcionar.
- En caso de robo o incendio, puedes recuperar todos los archivos suficientemente importantes a partir de copias almacenadas fuera del hogar.

11.2.5. Recursos para aprender más

- Para aprender a realizar copias de seguridad de dispositivos Android: https://www.xatakandroid.com/tutoriales/como-hacer-copia-seguridad-completa-movil-android.

- Para aprender a realizar copias de seguridad de dispositivos iOS: https://support.apple.com/es-es/HT203977.
- Para aprender a realizar copias de seguridad de Windows: https://support.microsoft.com/es-es/help/17127/windows-back-up-restore.
- Comparativa entre los principales almacenamientos en la nube: https://www.pcworld.es/mejores-productos/almacenamiento/servicios-almacenamiento-nube-3673539/.
- Como cifrar un disco duro con Windows 10: https://www.xataka.com/basics/como-cifrar-un-disco-duro-con-bitlocker-en-windows-10.

11.3. Gestión de contraseñas

11.3.1. Explicación problemática

La gran mayoría de los servicios web que utilizamos nos identifican mediante el uso de unas credenciales de usuario, consistentes en un nombre de usuario y una contraseña. Dichas credenciales tienen por objetivo conseguir que el servicio web pueda confirmar que somos nosotros los que efectivamente tratamos de acceder, pero hay muchas razones que llevan a que (en la práctica) sea menos seguro de lo que debería, bien porque dicha contraseña no esté protegiéndonos como debe, bien porque no sea tan privada como creemos.

- Incidentes de seguridad en el servicio web (por ejemplo, si son víctimas de un ataque) puede conllevar que nuestras credenciales se vean expuestas. Si reutilizamos la misma contraseña para otro servicio, un atacante puede hacerse pasar por nosotros en ese segundo servicio, aun cuando este no haya sufrido ningún incidente de seguridad.
- El uso de una contraseña insegura puede hacer que un atacante pueda hacer uso de fuerza bruta (probando millones o incluso miles de millones de contraseñas por segundo) hasta dar con ella.
- El almacenamiento incorrecto de la contraseña (en un post-it junto al ordenador, en un fichero de texto en nuestro escritorio, en un papel en la cartera) puede llevar a dos consecuencias indeseadas:
    - Cualquiera con acceso físico a ese papel o documento tiene acceso a nuestras contraseñas.
    - La pérdida de ese papel o documento nos lleva a perder las contraseñas que almacenaba, y con ello el acceso a los servicios que requerían esas credenciales.

11.3.2. Problemas frecuentes de seguridad y sus consecuencias

Los más normales en un entorno doméstico son:

- Incidentes de seguridad en el servicio web (por ejemplo, si son víctimas de un ataque) puede conllevar que nuestras credenciales se vean expuestas. Si reutilizamos la misma contraseña para otro servicio, un atacante puede hacerse pasar por nosotros en ese segundo servicio, aun cuando este no haya sufrido ningún incidente de seguridad.
- El uso de una contraseña insegura puede hacer que un atacante pueda hacer uso de fuerza bruta (probando millones o incluso miles de millones de contraseñas por segundo) hasta dar con ella.
- El almacenamiento incorrecto de la contraseña (en un post-it junto al ordenador, en un fichero de texto en nuestro escritorio, en un papel en la cartera) puede llevar a dos consecuencias indeseadas:
    - Cualquiera con acceso físico a ese papel o documento tiene acceso a nuestras contraseñas.
    - La pérdida de ese papel o documento nos lleva a perder las contraseñas que almacenaba, y con ello el acceso a los servicios que requerían esas credenciales.

11.3.3. Medidas de protección básicas

- En la medida de lo posible, utilizar una contraseña distinta para cada servicio web, de manera que un incidente de seguridad no comprometa a ningún otro.
- Uso de contraseñas seguras, con longitud mínima de 10-14 caracteres, bien generándolas con un gestor de contraseñas o mediante la concatenación de varias palabras que sean fáciles de recordar.
- Siempre que te ofrezcan la posibilidad de activar la autenticación multifactor en un servicio web, úsalo. Consiste en utilizar (además de la contraseña) otro elemento para identificarte: huella dactilar en dispositivo móvil, introducción de un código a recibir vía SMS, uso de una aplicación que genera un código de 6 dígitos válido solo durante 1 minuto, etc.
- Gestiona tus contraseñas de manera adecuada. Esto, salvo que dispongas de una memoria prodigiosa, significa utilizar un gestor de contraseñas que las almacene todas en una base de datos. Para proteger dicha base de datos se define una contraseña (que es necesario aprenderse de memoria y que nunca debe comunicarse a nadie ni utilizar

para nada más) que será necesario introducir cada vez que queramos consultar una contraseña. El fichero de la base de datos de contraseña debe tratarse como un archivo a proteger con la máxima atención, por lo que es necesario tenerlo en cuenta a la hora de realizar las copias de seguridad, y también a la hora de definir quien tiene acceso al mismo en nuestros sistemas, especialmente si disponemos de copias de seguridad de este en la nube.

- Las contraseñas no deben comunicarse nunca a nadie en ninguna circunstancia. Si recibimos una solicitud para que la entreguemos se trata de un ataque de phishing y debemos negarnos.
- Si vemos alguna cosa que nos hace sospechar de la página web del servicio (la URL no es la adecuada, tiene cambios visuales, etc.) no debemos introducir la contraseña ya que puede tratarse de un ataque.
- Si recibimos un correo que aparentemente viene del proveedor de servicio y se nos ofrece una casilla para entrar directamente en el servicio (con el pretexto de ahorrarnos tiempos) o se nos ofrece un enlace al servicio, nunca debemos introducir las credenciales. Si queremos entrar al servicio (a fin de validar que la información que se había incluido en el correo era cierta), procederemos a abrir un navegador y teclear la dirección del servicio, de manera que nos aseguremos que introducimos la contraseña en el servicio legítimo y no en uno que pudiera estar controlado por un atacante.

11.3.4. Comprobación rápida

Esta área se encuentra adecuadamente protegida si:

- Utilizas una contraseña distinta para cada servicio.
- Sabes que significa que una contraseña sea segura, y las tuyas lo son.
- Almacenas las contraseñas en un gestor de contraseñas, y nunca en un papel.
- Sabes que es la autenticación multifactor y la utilizas para proteger los servicios más importantes, como por ejemplo los bancarios o el correo.
- Sabes que nunca hay que dar las contraseñas a nadie ni introducirlas en una página web si sospechas que no es la legítima.

11.3.5. Recursos para aprender más

- Generación de contraseñas seguras: https://support.mozilla.org/es/kb/crear-contrasenas-mas-seguras-para-mantener-tu-identidad-a-salvo.

- Gestor de contraseñas: https://www.xataka.com/basics/gestores-contrasenas-que-cuales-populares-como-utilizarlos.
- Autenticación multi-factor: https://es.wikipedia.org/wiki/Autenticaci%C3%B3n_de_m%C3%BAltiples_factores.
- Autenticación multi-factor mediante App: https://es.wikipedia.org/wiki/Google_Authenticator.

11.4. Usar programas con vulnerabilidades

11.4.1. Explicación problemática

A la hora de ejecutar un programa, es importante que cumpla con la funcionalidad que esperamos de él, pero es igual de importante que lo haga de una manera segura, sin poner en riesgo nuestra seguridad.

En ocasiones los usuarios nos olvidamos de este segundo aspecto e instalamos cualquier programa que prometa realizar una función determinada sin pararnos a pensar en las implicaciones que puede tener.

11.4.2. Problemas frecuentes de seguridad y sus consecuencias

Hay muchos, y muy variados, problemas asociados al uso de programas vulnerables:

- El uso de programas piratas puede hacernos creer que nos ahorramos un dinero (dado que no pagamos el dinero de la licencia) pero, además de ilegal, muchas veces son versiones creadas por los atacantes para incorporar vulnerabilidades que les hagan poder controlar nuestros dispositivos y lograr acceso a nuestros datos personales.
- El uso de versiones desfasadas de los programas (nuevamente muy habitual en el caso de los programas piratas al no tener acceso a las últimas versiones presentadas por el fabricante) conlleva que presenten problemas de seguridad que ya han sido solucionados en la última versión de este. Esto es mucho más grave de lo que parece, ya que dichos problemas de seguridad son conocidos por los atacantes, por lo que pueden valerse de estos para controlar nuestros dispositivos y acceder a nuestros datos personales.
- Unos programas en los que no solemos fijarnos son aquellos que controlan ciertos dispositivos que no nos parecen un ordenador, como pueden ser los televisores y los

routers de conexión a Internet, pero que en el fondo se comportan de la misma manera y se encuentran expuestos a la misma problemática.

11.4.3. Medidas de protección básicas

Para protegerse adecuadamente, las reglas a seguir son las siguientes:

- Debemos usar programas originales y, siempre que nos ofrezca la posibilidad, activar las actualizaciones automáticas. El sistema operativo es el primer programa en el que tenemos que fijarnos, instalando solamente copias legales de manera que podamos activar todas las medidas de seguridad que vienen con este.
- Cuando no existan la posibilidad de actualizar automáticamente, debemos comprobar periódicamente la existencia de actualizaciones. Esto es muy habitual en los televisores y los routers de conexión a Internet. Es por ello que, a la hora de comprar dispositivos electrónicos, es muy importante verificar primero que disponen de un buen servicio técnico que vaya sacando versiones nuevas para mejorar la funcionalidad y seguridad de nuestro dispositivo, y que proporcione soporte para los usuarios que necesiten ayuda con la actualización.
- A la hora de instalar programas, es importante realizarlo solamente desde fuentes oficiales, y no proseguir con la instalación si algún elemento que nos hace sospechar, como pueden ser los mensajes de error relacionados con la seguridad durante el proceso de instalación. Las fuentes de máxima confianza son aquellas gestionadas por los responsables de los distintos sistemas operativos y dispositivos
    - Android: “Google Play”.
    - iOS: “Apple Store”.
    - Windows: “Windows Store”

11.4.4. Comprobación rápida

Esta área se encuentra adecuadamente protegida si:

- Utilizas copias legales de los programas, descargadas desde Google Play, Apple Store, Windows Store o la web del fabricante.
- Tienes activadas las actualizaciones automáticas en todos tus dispositivos , y actualizas los programas cuando te lo ofrecen.

11.4.5. Recursos para aprender más

- Para configurar la actualización automática de las aplicaciones en Android: https://www.xataka.com/basics/como-desactivar-las-actualizaciones-automaticas-de-las-aplicaciones-de-android-en-google-play.
- Para configurar la actualización automática de las aplicaciones en iOS: https://support.apple.com/es-mx/HT202180.
- Para configurar la actualización automática de las aplicaciones en Windows 10: https://www.pcworld.es/tutoriales/software/configurar-actualizaciones-automticas-windows-10-3675705/.
- Para conocer como actualizar la versión del programa que controla un dispositivo que hemos comprado nosotros (por ejemplo, la televisión), lo más sencillo es acudir al manual de servicio de este o a la página web del fabricante donde podremos contactar con el servicio de soporte.
- Para conocer como actualizar la versión del programa que controla un dispositivo que no hemos comprado nosotros (por ejemplo, el router que nos entrega la compañía con la que tengamos contratado el acceso a Internet), lo más sencillo es acudir a la página web de la compañía que nos ofrece el dispositivo como parte del servicio, y acceder a su servicio de atención al cliente para preguntar por dichas actualizaciones.

11.5. Configuración insegura

11.5.1. Explicación problemática

Cuando instalamos y configuramos los distintos programas informáticos, estos suelen venir configurados de la manera que garantice la mayor compatibilidad con los usuarios, de cara a simplificar la instalación. El otro lado de la moneda es que dichas configuraciones suelen dejar muchas “puertas abiertas” que aumentan las probabilidades de que un atacante sea capaz de aprovechar alguna de ellas para poder acceder a nuestros sistemas y a nuestros datos.

Es responsabilidad de los usuarios asegurarse que configuran todos sus equipos balanceando la sencillez de uso con el riesgo que quieran correr.

11.5.2. Problemas frecuentes de seguridad y sus consecuencias

Hay varios problemas importantes a destacar:

- Dejar instalada funcionalidad que ya no utilizamos deja nuestros equipos vulnerables a cualquier ataque específico que pueda existir contra dicha funcionalidad. Puede parecer que es el mismo caso que para aquellos programas o funcionalidades que si usamos (ya que la problemática es la misma), pero es fundamental entender la diferencia intrínseca de que en este segundo caso estamos aumentando el riesgo a cambio de algo que necesitamos o queremos usar, mientras que en el caso de funcionalidad que ya no utilizamos nos estamos exponiendo más a cambio de nada.
- Casi todos los dispositivos electrónicos modernos (televisores, routers de acceso a internet, ordenadores, teléfonos inteligentes, tabletas, etc.) disponen de muchísimas funcionalidades de seguridad que es necesario configurar adecuadamente a fin de que funcionen como han sido diseñados y no se conviertan en elementos neutros desde el punto de vista de la seguridad (es decir, que ni mejoran ni empeoran la misma) o incluso se conviertan en un 'agujero' de seguridad en los casos más extremos.

11.5.3. Medidas de protección básicas

La lista de medidas sugeridas no puede ser considerada como exhaustiva, aunque sí como un buen inicio, debiendo acudir a los recursos indicados en la sección 'recursos para aprender más' para seguir mejorando la configuración de nuestros dispositivos.

En primer lugar, citaremos algunas recomendaciones generales, pasando a continuación a las medidas más importantes en los principales tipos de dispositivos.

Recomendaciones generales:

- Los programas tienen un 'ciclo de vida' y es necesario cuidar de ellos en sus distintas etapas:
    - Antes de instalarlo, debemos verificar los comentarios sobre el mismo a fin de poder identificar si va a sernos útil para la tarea que queremos realizar. Al mismo tiempo, caso de haber más de una opción disponible, debemos fijarnos en el soporte ofrecido por el fabricante de este, a fin de tratar de utilizar aquellos programas que dispongan de nuevas versiones periódicamente.
    - Durante la instalación, esto aplica principalmente a los programas instalados en un ordenador, hay que leer la documentación y entender las implicaciones de seguridad que tiene cada una de las opciones habilitadas. Como regla general, conviene activar únicamente aquella funcionalidad que sepamos seguro que vamos a necesitar. Al mismo tiempo, es necesario interesarse por las opciones

de seguridad que pueda tener el programa y tratar de activar (y configurar correctamente) la mayor parte de estas.
    - Mientras el programa nos es útil, debemos actualizarlo periódicamente con las nuevas versiones que vayan surgiendo, y debemos prestar atención a los avisos de seguridad que pueda mostrarnos. Caso de tener dudas, podemos acudir al servicio de soporte del fabricante para aclarar el significado de los mensajes.
    - Una vez no necesitamos más el programa, es preferible copiar aquellos datos relevantes que hayamos guardado en el mismo y proceder a borrarlo.
- Todo dispositivo conectado a Internet puede ser objetivo de ataque, por lo que es necesario prestar atención a todo dispositivo que conectemos a nuestra WiFi, o también mediante cable al router. Esto incluye televisores, consolas y cualquier electrodoméstico inteligente. Queda fuera del alcance de esta guía poder incluir instrucciones detalladas para cada uno de los casos, pero la manera de actuar en general consiste en
    - Mirar si el manual de usuario del dispositivo incluye información relevante para la seguridad, como pueda ser que funciones de seguridad tiene el dispositivo y como configurarlas correctamente.
    - Caso de no encontrarlo, acudir a la página web del fabricante del dispositivo para buscar esta misma información.
    - Si el fabricante no dispone de dicha información, o está en inglés y no somos capaces de entenderlo, se puede acudir a un buscador e introducir “como proteger” seguido del nombre de dispositivo, aunque esta tercera opción es recomendable solo cuando se tenga cierta soltura con la configuración de dispositivos.

Recomendaciones por dispositivo

- Ordenadores Windows. Las instrucciones incluidas se refieren a un Windows 10
    - Como se ha comentado en otros apartados, instalar una licencia legal de Windows y mantenerlo al día de actualizaciones.
    - Desinstalar todos aquellos programas que no vayamos a necesitar.
    - Lanzar la configuración de Windows pulsando ‘tecla de Windows + I’. Una vez allí
        - Pulsar la opción Cuentas
            - Ir a ‘Opciones de inicio de sesión’ y configurar que se requiera el inicio de sesión cuando el PC se activa después de haber

estado en suspensión. Si queremos cambiar la contraseña de nuestra cuenta por una segura o cambiar las preguntas de seguridad también se hace desde este punto. Una última funcionalidad relevante en este apartado es la posibilidad de definir unas preguntas de seguridad que nos permitan recuperar la contraseña si la olvidamos, que es una funcionalidad que deberíamos no utilizar si disponemos de un gestor de contraseñas.

- Ir a 'Familia y otros usuarios' y crear una cuenta distinta para cada usuario que vaya a utilizar el ordenador. Esto nos permitirá proteger ciertas partes del ordenador para que solo estén disponibles a ciertos usuarios o para proteger a los menores activándoles filtros de acceso a determinados contenidos.

- Pulsar la opción Aplicaciones
  - En 'Aplicaciones y características' se puede forzar a que todos los usuarios solamente puedan instalar aplicaciones desde la tienda de aplicaciones de Microsoft, o bien relajar la política y al menos advertir cuando se trate de instalar una aplicación que tenga otro origen. Pulsando en 'Administrar funciones opcionales' podemos desinstalar aquellos elementos que vienen con Windows pero que no necesitamos.
  - En 'Aplicaciones para sitios web' se debe desmarcar todos aquellos programas que no queramos lanzar directamente desde las páginas web. Salvo que tengas un motivo para lo contrario, deberías desactivarlos todos.
  - En 'Inicio' se puede ver que programas se lanzan de manera automática cada vez que se arranca Windows. Es conveniente repasar la lista de vez en cuando y desactivar todos aquellos programas que no nos sean relevantes. Varios de los programas son necesarios para que funcione correctamente el ratón o el audio (por poner dos ejemplos) por lo que hay que acudir al navegador para buscar que hacen los programas que queramos desactivar.
- Pulsar Cortana

- Cortana es el asistente de voz de Windows, lo que significa que el ordenador se encuentra escuchando todo el rato lo que decimos. Si no se desea hacer uso de esta funcionalidad es necesario desactivar todas las maneras de activarlo que se incluyen en el apartado 'Hablar con Cortana'.
- En 'Permisos e historial' puedes gestionar las opciones de privacidad de Cortana. Salvo que sea una funcionalidad que necesites, lo mejor es desactivar los distintos historiales a fin de que el ordenador no almacene información sobre lo que hayas buscado.

- Apartado de Privacidad
  - En el apartado general se indica a Windows que datos debe compartir con las distintas aplicaciones a fin de mostrarnos anuncios relevantes. Es decisión personal de cada uno elegir si prefiere dar más información para que los anuncios sean relevantes o si se quiere desactivar toda compartición de información e ignorar completamente los anuncios irrelevantes.
  - En el apartado de Voz, puedes desactivar todo reconocimiento de voz para asegurar que Windows no graba sonidos con el micrófono.
  - En 'Comentarios y diagnósticos' se debe asegurar que los datos de diagnóstico compartidos son básicos, a fin de evitar que se den demasiados datos a Microsoft con cada reporte de errores.
  - En 'Historial de actividad' se debe desmarcar que se envíe a Microsoft. Nuevamente, es personal la decisión de almacenar el historial local o no, según lo encontremos útil.
  - Por último, para cada uno de los permisos básico (uso de micrófono, uso de la cámara, etc.) se puede activar o desactivar a nivel general. Si se activa, se puede seleccionar a que aplicaciones se les ha dado permiso para usar dicho recurso. Conviene repasar periódicamente la lista para estar seguros de que ninguna aplicación no deseada tiene acceso a los mismos.
- El apartado de 'Actualización y seguridad' es el más importante

        - En ‘seguridad de Windows’ debemos ver todos los puntos con una marca blanca sobre un círculo verde, que nos indica que está configurado correctamente. Si en algún caso no es así, podemos clicar en ese elemento para ver qué es lo que falta por realizar o activar. Esta es la acción más relevante desde el punto de vista de la seguridad del sistema, ya que activa las principales funciones de seguridad de Windows que proporcionan una seguridad relativamente buena frente a virus, ataques que nos lleguen desde Internet y otras amenazas.
        - Desde ‘Copia de seguridad’ es posible realizar copias de seguridad del ordenador en una unidad de disco duro USB.
    - Trata de minimizar el número de extensiones y plugins que instalas en el navegador, ya que dichos complementos pueden tener acceso a las comunicaciones que realices desde el mencionado navegador, por lo que solo hay que instalar las imprescindibles y siempre que se tenga un buen motivo para ello.
- Dispositivos Android
    - Mantén tu dispositivo actualizado a la última versión disponible. Esto quiere decir que debes aceptar las actualizaciones de seguridad que te ofrece el sistema operativo tan pronto como sea posible.
    - No intentes instalar tiendas de aplicaciones distintas a las que vienen con el teléfono.
    - Activa las actualizaciones automáticas de las aplicaciones.
    - Encripta el dispositivo.
    - Configura una contraseña para la pantalla de bloqueo, y esta para que salte automáticamente tras unos minutos de inactividad. Recuerda la información recomendada incluida en el apartado de gestión de las contraseñas.
    - Apaga el bluetooth, NFC y la WiFi cuando no los estés usando.
    - Configura Google Play para que pida la contraseña para cada compra.
    - Desactiva la ubicación por GPS cuando lo no necesites.
- Dispositivos iOS
    - Mantén tu dispositivo actualizado a la última versión disponible. Esto quiere decir que debes aceptar las actualizaciones de seguridad que te ofrece el sistema operativo tan pronto como sea posible.

- No intentes instalar aplicaciones desde fuera de la Apple Store.
- Activa las actualizaciones automáticas de las aplicaciones.
- Encripta el dispositivo.
- Configura una contraseña para la pantalla de bloqueo, y esta para que salte automáticamente tras unos minutos de inactividad. Recuerda la información recomendada incluida en el apartado de gestión de las contraseñas.
- Apaga el bluetooth, AirDrop y la WiFi cuando no los estés usando.
- Configura Apple Store para que pida la contraseña para cada compra.
- Desactiva la ubicación por GPS cuando lo no necesites.
- Activa la autenticación de doble factor para proteger tu cuenta de Apple.

- Router de conexión a Internet. Las medidas indicadas son generales, debiendo acudir a la documentación del fabricante (o al servicio técnico de nuestro proveedor de Internet) para obtener instrucciones detalladas
  - Actualiza el firmware a la última versión, y comprueba periódicamente que no existen versiones más modernas sin actualizar. Si es posible, configura las actualizaciones para que se realicen de manera automática.
  - Los routers vienen con una pegatina con las credenciales por defecto a utilizar para poder entrar a la consola de administración. Es conveniente modificar dicha contraseña, a fin de evitar que sea conocida por alguien que no seamos nosotros.
  - Si no utilizas WiFi, desactívalo. Si lo utilizas, establece una contraseña de WiFi segura y activa el sistema de seguridad WPA2 (o mejor WPA3 si el router dispone de este), y nunca utilices WPA.
  - Cambia el SSID por defecto por uno que no signifique nada. Esto es debido a que da información sobre tu operador y/o el modelo de router, lo que facilita a un atacante saber que problemas de seguridad debe buscar.
  - Desactiva el acceso remoto a la administración del router, de manera que para poder entrar a la consola de administración haya que estar conectado al mismo (vía cable o WiFi).
  - Desactiva UPnP, o Universal Plug and Play, que hace que el router automáticamente permita la conexión a cualquier dispositivo que se conecte a la red a través de los puertos de conexión específicos que necesite. Si lo desactivas, tendrás que manualmente abrir los puertos cuando quieras utilizar protocolos como BitTorrent, pero evitarás muchos problemas de seguridad.

11.5.4. Comprobación rápida

Esta área se encuentra adecuadamente protegida si:

- Instalas solo aquellos programas legales que necesitas, revisas su configuración para habilitar solo aquello que necesitas, los actualizas cuando salen nuevas versiones y los desinstalas cuando los necesitas más.
- Para cada dispositivo conectado a Internet (televisor, router, teléfonos, ordenador, etc.) revisas su configuración para habilitar solo lo que necesitas, buscas y sigues las instrucciones específicas para protegerlo, actualizas a la última versión disponible cuando te lo ofrecen.
- Sabes el estado actual de tus dispositivos, y tienes confianza en que están convenientemente configurados y protegidos.

11.5.5. Recursos para aprender más

- Configurar la privacidad en Windows 10: https://www.osi.es/es/actualidad/blog/2016/12/15/configurando-tu-privacidad-en-windows-10.
- Guías de seguridad del centro criptológico nacional para dispositivos:
    - Windows: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2392-ccn-stic-599b-seguridad-en-windows-10-cliente-independiente/file.html
    - Android: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2733-ccn-stic-453c-seguridad-en-android-5-x/file.html
    - iOS: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7175-guias-practicas-de-seguridad-en-dispositivos-moviles-iphone-ios-11-x-y-ios-12-x.html.
- Copias de seguridad en Windows 10: https://www.xataka.com/basics/copias-seguridad-windows-10-sirven-que-tipos-hay-como-se-hacen.
- Como encriptar un dispositivo Android: https://www.xatakandroid.com/seguridad/como-encriptar-tu-movil-android-y-que-consigues-con-ello.
- Establecer bloqueo de pantalla en dispositivos Android: https://support.google.com/nexus/answer/9079129?hl=es.

- Configurar Android para que solicite contraseñas para las compras: https://support.google.com/googleplay/answer/1626831?hl=es.
- Lista de seguridad de sistemas Android: https://www.ocu.org/tecnologia/telefono/noticias/ajustes-seguridad-movil-android.
- Actualizaciones automáticas en dispositivos Android: https://support.google.com/googleplay/answer/113412?hl=es.
- Autenticación de doble factor para el ID de Apple: https://support.apple.com/es-es/HT204915.
- Copias de seguridad de iOS: https://support.apple.com/es-es/HT203977.
- Ajustes de privacidad y seguridad a revisar en iOS 12: https://luisgyg.com/privacidad-y-seguridad-ios-12/.
- Configuraciones de seguridad para Android e iOS: https://blog.sucuri.net/espanol/2017/08/seguridad-para-dispositivos-ios-android.html.
- Proteger la red WiFi: https://www.osi.es/es/protege-tu-wifi.
- Configuración del router de Movistar: http://www.movistar.es/particulares/internet/adsl-fibra-optica/clientes/configuracion-routers-portal-alejandra/.
- Configuración de los distintos routers de Vodafone: https://ayudacliente.vodafone.es/particulares/internet-movil-fijo/wifi/configuracion-de-modems-y-routers/.
- Configuración de los distintos routers de Orange: https://ayuda.orange.es/dispositivos-y-routers/.

11.6. Educación

11.6.1. Explicación problemática

La mayoría de los problemas de seguridad se deben al eslabón más débil de la cadena: los propios usuarios. Esto es verdad en todos los ámbitos, pero particularmente en los entornos domésticos donde muchas veces se carece de la información suficiente para poder tomar las decisiones adecuadas.

Esta brecha de información, lejos de ir reduciéndose con el tiempo, suele aumentar debido al creciente número de dispositivos, al creciente tipo de ataques y a que los atacantes no

disminuyen su empeño (al fin y al cabo, es su trabajo), mientras que los usuarios solemos acomodarnos y dejamos de aprender.

11.6.2. Problemas frecuentes de seguridad y sus consecuencias

Las principales áreas donde es necesario tener conocimientos de seguridad, aunque a la fuerza hay otras que se han quedado fuera de la misma:

- Comercio electrónico.
- Gestión de la privacidad en Internet.
- Conexión a Internet de manera segura.
- Redes sociales

Las consecuencias son tan variopintas como podamos imaginar, por lo que solo se puede considerar esta lista como ejemplos de lo que puede llegar a sucedernos:

- Pérdidas económicas, tanto por fraude como por robo del dinero depositado en nuestras cuentas bancarias.
- Pérdida de nuestra información personal o divulgación de esta a usuarios no autorizados.
- Problemas con la justicia si un atacante comete delitos electrónicos desde nuestros dispositivos.

El motivo de presentar estos ejemplos no es alarmar, sino concienciar de las graves consecuencias que puede tener descuidar la seguridad digital.

11.6.3. Medidas de protección básicas

Si bien las medidas, a nivel general, son muy fáciles de explicar, conllevan una dificultad y esfuerzo por parte de los usuarios.

- Mantenerse al día de las alertas de seguridad: https://www.osi.es/es/actualidad/avisos.
- Ante sospecha de fraude, investiga desde el navegador los mensajes que recibes o ves.
- Investiga sobre aquella acción que quieras realizar, hasta tener una certeza suficiente de que el servicio al que tratas de conectarte es legítimo.
- No te conectes a redes WiFi abiertas, ya que puede permitir el acceso a los datos que encamines a través de ella a quien controle dicha red.

- Accede a sitios de confianza para incrementar tus conocimientos de seguridad, empezando por aquellas actividades que realices más frecuentemente.
- De la Oficina de Seguridad del Internauta, lee los siguientes apartados:
    - Se cauto con las redes públicas: https://www.osi.es/es/wifi-publica.
    - Cuida tu privacidad: https://www.osi.es/es/tu-informacion-personal.
    - Como proteger la privacidad en los navegadores: https://www.osi.es/es/navegadores.
    - Compras online: https://www.osi.es/es/pagos-online y https://www.osi.es/es/pagos-online.
    - Redes sociales: https://www.osi.es/es/redes-sociales.
    - Mensajería instantánea: https://www.osi.es/es/mensajeria-instantanea.
    - Correo electrónico: https://www.osi.es/es/correo-electronico.
    - Juegos online: https://www.osi.es/es/juegos-online.
    - Tu información en la nube: https://www.osi.es/es/tu-informacion-en-la-nube.
    - Webs de descarga: https://www.osi.es/es/webs-de-descarga.
    - Casinos y apuestas: https://www.osi.es/es/casinos-y-apuestas.
    - Ataque de phishing: https://www.osi.es/es/banca-electronica.
    - Tiendas online fraudulentas: https://www.osi.es/es/tiendas-online-fraudulentas.
    - Estafas en alquileres: https://www.osi.es/es/estafas-alquileres.
    - Falsas ofertas de empleo: https://www.osi.es/es/falsas-ofertas-empleo.
    - Fraude online: https://www.osi.es/es/fraude-online.

11.6.4. Comprobación rápida

Esta área se encuentra adecuadamente protegida si:

- Te sientes cómodo en Internet y seguro comprando y realizando operaciones bancarias, ya que sabes detectar los distintos problemas y estafas.
- Sabes proteger tu privacidad en la nube, redes sociales y navegando por Internet.
- Sabes lo que significa y como debes protegerte ante amenazas como: phishing, fraude online, ataques de ingeniería social, etc.
- Estás al día de los nuevos ataques e informaciones relacionadas con la ciberseguridad en el hogar, bien porque leas noticias relacionadas o porque estés suscrito a algún servicio de alertas.

11.6.5. Recursos para aprender más

- Guías específicas del Centro Criptológico Nacional: https://www.ccn-cert.cni.es/guias/indice-de-guias.html.
- Guía de privacidad y seguridad en Internet: https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet.
- Guía de compra segura en Internet: https://www.osi.es/es/actualidad/blog/2017/12/19/te-interesa-estrenamos-guia-sobre-compra-segura-en-internet.

11.7. Menores en el hogar

11.7.1. Explicación problemática

Los menores en el hogar son fuente de pequeñas problemáticas que nos llevan a tener que adaptar nuestra forma de hacer las cosas de manera que nos protejamos ante los errores involuntarios que cometen, y de los cuales expondremos unos cuantos en la sección siguiente.

11.7.2. Problemas frecuentes de seguridad y sus consecuencias

Todo el mundo con menores en casa ha experimentado, en mayor o menor medida, alguno de los problemas descritos a continuación, aunque no debemos conformarnos con controlar esos puntos, dado que los niños tienen la capacidad de sorprendernos y salir por el sitio menos pensado:

- Los niños no disponen de 'filtros' a la hora de compartir la información que conocen. Es normal que nos avergüencen delante de conocidos y desconocidos contando alguna intimidad sin ninguna consecuencia más allá del sonrojo que nos produce. Esta cualidad, sin embargo, puede volverse muy preocupante si la naturaleza de la información que conocen no es tan inocua para nosotros, ¿qué pasaría si un niño conoce y divulga las credenciales de acceso a nuestra cuenta bancaria?
- Cuando un niño quiere conseguir algo, no repara en que otro perjuicio puede conllevar su acción. Cuando se comparte un dispositivo con ellos, por ejemplo, el teléfono móvil en una comida para que puedan ver sus dibujos preferidos y dejarnos comer tranquilos, es habitual que se salgan de la aplicación que les habíamos indicado y tanto accedan a la información almacenada en el dispositivo como usen el navegador para poder

acceder a Internet sin filtros. De la misma manera, es habitual que desactiven sin querer la WiFi y que eso nos lleve a agotar los datos del mes y nos quedemos sin datos hasta que comience el siguiente ciclo de facturación.

- Es habitual que, involuntariamente, desconfiguren o desconecten los distintos aparatos que podamos tener por casa.

11.7.3. Medidas de protección básicas

Nada sustituye al sentido común ni al conocimiento que tenemos de nuestros hijos, dado que los problemas suelen ser recurrentes y tendremos que adaptarnos a la forma de comportarse de estos, pero algunas recomendaciones generales son:

- Hay que tener mucho cuidado con cualquier información que se dice en presencia de los niños, o que se deja al alcance. La única información que sabemos seguro que no va a compartir es aquella de la que no disponen.
- Cuando se deja un dispositivo de un adulto al niño
    - Hay que procurar limitarlo de tal manera que solo pueda ejecutarse la aplicación que nosotros hayamos seleccionado.
    - Hay que tratar de comprobar cada cierto rato que siga utilizándolo para lo que se lo habíamos dejado.
    - Cuando nos devuelve, hay que hacer ciertas comprobaciones básicas para evitar que nos haya modificado alguna configuración, como pudiera ser desactivar la WiFi.
- En la medida de lo posible, debemos configurar nuestros dispositivos con dos cuentas, y siempre que se lo dejemos debemos cambiar a la cuenta sin privilegios, en la que solo permitiremos la ejecución de aquellos programas adecuados al menor. Si esto no es posible, hay que tratar de proteger las distintas aplicaciones con nuestra huella digital o un PIN.
- Para facilitar la reconfiguración de lo que puedan desconfigurar, es necesario tener una copia de todos aquellos datos que puedan sernos útiles: contraseñas, esquemas de conexión, etc.
- Controlar y limitar el uso a través de herramientas de control parental: https://www.is4k.es/de-utilidad/herramientas.

11.7.4. Comprobación rápida

Esta área se encuentra adecuadamente protegida si:

- Proteges los dispositivos usados por los menores, de manera que no tengan acceso a la información sensible almacenada en los mismos ni tienen permiso para realizar cambios perjudiciales.
- En el caso de que el dispositivo resulte dañado, o desconfigurado, eres capaz de restaurarlo.
- El uso de los dispositivos está controlado y limitado mediante herramientas de control parental.

11.8. Educación y protección de los menores

11.8.1. Explicación problemática

Es fácil darse cuenta de que los miembros más desprotegidos de cualquier hogar son los menores que, a la falta de conocimientos sobre seguridad digital, suman desconocimiento en general sobre la clase de gente que puede haber en el mundo y no están preparados para su exposición a muchos tipos de contenidos.

Al mismo tiempo, no son conscientes de las implicaciones de sus actos, por lo que es necesario prestarles una especial atención, además de guiarles en su aprendizaje digital. Muchas veces confundimos la facilidad que tienen para todo lo electrónico (por algo se dice que son nativos digitales) con un conocimiento de lo que están haciendo, lo que nos lleva a malinterpretar que su aprendizaje al respecto está siendo satisfactorio, pero no debemos engañarnos, eso solamente es un reflejo que los programas y los dispositivos hoy en día son muy intuitivos, además de la tenacidad que puede llegar a tener un niño cuando tiene algo que le motiva.

11.8.2. Problemas frecuentes de seguridad y sus consecuencias

Son muchos y muy graves los problemas que los menores pueden tener con el uso de las nuevas tecnologías:

- Ciberacoso escolar
- Acceso a contenido inapropiado
- Conexión con comunidades peligrosas

- Sexting
- Problemas de privacidad
- Uso excesivo de pantallas y nuevas tecnologías

11.8.3. Medidas de protección básicas

Disponemos de amplia información sobre todos los puntos problemáticos identificados, así como de herramientas, alertas, como educar a los menores en el uso de la tecnología y otros muchos materiales en la página de Internet Segura 4 KiDS: https://www.is4k.es

Cada padre debe entrar en dicha página y valorar todos los contenidos que son relevantes en su caso, pues va a depender de factores tan variopintos como la edad de los menores o los conocimientos del progenitor, por lo que esta guía no va a facilitar un guion de navegación que pueda causar la omisión de un punto relevante.

No hay que olvidarse de dar un vistazo a las múltiples guías que hay disponibles para el uso seguro de juguetes conectados, el ciberbullying, convivir con las pantallas o evitar la adicción a los videojuegos (entre otros temas), que debemos consultar a modo introductorio o si tenemos identificado un posible problema al respecto.

11.8.4. Comprobación rápida

Esta área se encuentra adecuadamente protegida si:

- Estás suficientemente formado en aquellos problemas relevantes para la franja de edad de los menores que haya en el hogar, como ciberacoso escolar, uso excesivo de las pantallas o sexting, y acudes periódicamente a Internet Segura 4 KiDS u alguna otra web específica.
- Transmites estos conocimientos a los menores en el hogar, y eres capaz de tener un diálogo abierto con ellos respecto a estos aspectos, dado que el verdadero objetivo es prepararlos a ellos para que puedan utilizar Internet de manera responsable y segura.

12. Resultados

El presente TFM ha dado como resultado dos elementos principales:

- Por un lado, el análisis formal recogido en este documento.
- Por otro, la "Guía Práctica de Ciberseguridad en el Hogar", cuyo contenido se encuentra incluido dentro de este documento, pero que está preparada para poder ser entregada a los usuarios finales, de manera que puedan aprender a protegerse adecuadamente de las amenazas que les rodean en el entorno digital.

A nivel temporal, el desarrollo del TFM se ha realizado dentro de los plazos estimados en el apartado de Planificación para la entrega de este en la convocatoria de junio, lo que ha supuesto un gran esfuerzo pero que sin duda ha merecido la pena, tanto por el aprendizaje personal como por el resultado obtenido.

13. Conclusiones y trabajo futuro

A la vista de los comentarios recogidos de los usuarios con los que he ido compartiendo los apartados de la guía, el objetivo principal del trabajo se ha alcanzado con éxito ya que, si bien no todos son capaces de entender todo el contenido, sí que me indican que les sirve como punto de consulta para ver qué es lo que deben hacer y que se plantean ir realizando y aprendiendo poco a poco. Por lo tanto, me quedo muy satisfecho con la acogida que me han brindado, aunque siempre cabe matizarlo dado que estas personas son amigos y familiares, lo que ha influido positivamente en su actitud ante mis preguntas y en la voluntad que han demostrado para implicarse en la tarea.

Respecto a los objetivos secundarios, estimo que también han sido alcanzados durante la elaboración del presente trabajo y de la guía resultante.

En ambos casos, por supuesto, el contenido de este trabajo no puede considerarse como el último paso que se puede dar al respecto, sino más como un punto intermedio en el que ya se ha recorrido mucho camino, pero a la vez se abren muchas posibilidades por donde se puede continuar la labor, como pueden ser:

- Generar guías para usuarios intermedios / avanzados.
- Añadir nuevos recursos.
- Traducir a idiomas.
- Mejorar el formato de la guía, unificando el tamaño de cada sección, añadiendo diagramas, etc.
- Validar con más usuarios finales para adaptar mejor el contenido.
- Bajar el umbral máximo de error de medio a bajo o muy bajo.
- Preparar videotutoriales donde se muestre paso a paso como realizar las distintas configuraciones.
- Conseguir una difusión de la guía generada, de manera que se maximice su impacto positivo en la sociedad.
- Presentar el contenido en charlas para concienciar a los padres y docentes sobre la problemática.

Referencias

1. Magerit – Metodología de Análisis y gestión de riesgos de los sistemas de información. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XI6QGbh7nIU.
2. Magerit – Wikipedia. Disponible en: https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa).
3. Esquema nacional de seguridad - Real Decreto 3/2010. Disponible en: http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2010-1330.
4. Introducción – Tema 3 Sistemas de clasificación de la información – Sistemas de Gestión de la Seguridad. Disponible en: https://moodle2018-19.ua.es/moodle/mod/page/view.php?id=32489.
5. Salvaguardas – Tema 4 Análisis de Riesgos – Sistemas de Gestión de la Seguridad. Disponible en: https://moodle2018-19.ua.es/moodle/mod/page/view.php?id=34753&forceview=1.
6. Una al día – Boletín de noticias de HISPASEC SISTEMAS S.L. Disponible en: https://unaaldia.hispasec.com/.
7. Instituto Nacional de Ciberseguridad, página web disponible en: https://www.incibe.es/.
8. Instituto Nacional de Ciberseguridad, página de la Wikipedia disponible en: https://es.wikipedia.org/wiki/Instituto_Nacional_de_Ciberseguridad.
9. Oficina de Seguridad del Internauta, página web disponible en: https://www.osi.es/es.
10. Internet Segura For Kids, página web disponible en: https://www.is4k.es/.
11. Guía de privacidad y seguridad en Internet – INCIBE. Disponible en: https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet.
12. Guía de compra segura en Internet – INCIBE. Disponible en: https://www.osi.es/sites/default/files/docs/guia_compra_segura_internet_web_vfinal.pdf.
13. Fichas prácticas compra segura en Internet – INCIBE. Disponible en: https://www.osi.es/sites/default/files/docs/fichas_compra_segura_internet_web_vfinal.pdf.

14. Guía de juguetes conectados – INCIBE. Disponible en: https://www.is4k.es/sites/default/files/contenidos/materiales/Campanas/is4k_guiajuguetesconectados_v1.pdf
15. Guía de mediación parental – INCIBE. Disponible en: https://www.is4k.es/sites/default/files/contenidos/herramientas/is4k_guia_mediacion_parental_internet.pdf.
16. Vive Internet Seguro – OCU y Google. Disponible en: https://www.ocu.org/viveinternetseguro/.
17. Impacto – Tema 4 Análisis de riesgos – Sistemas de Gestión de la Seguridad. Disponible en: https://moodle2018-19.ua.es/moodle/mod/page/view.php?id=34392&forceview=1.
18. Riesgo – Tema 4 Análisis de riesgos – Sistemas de Gestión de la Seguridad. Disponible en: https://moodle2018-19.ua.es/moodle/mod/page/view.php?id=34393&forceview=1.